ZyWALL P1

Internet Security Appliance

User's Guide

Version 4.04
2/2008
Edition 1

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyWALL using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide
  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help
  Embedded web help for descriptions of individual screens and supplementary information.
- Command Reference Guide
  The Command Reference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the ZyWALL.

It is recommended you use the web configurator to configure the ZyWALL.

- Supporting Disk
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your ZyWALL.

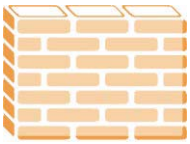
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The ZyWALL P1 may be referred to as the "ZyWALL", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyWALL icon is not an exact representation of your ZyWALL.

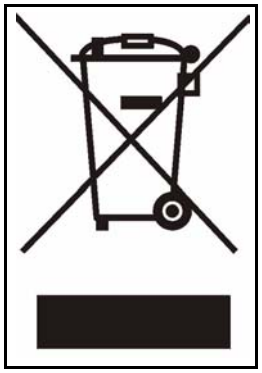
ZyWALL	Computer	Notebook computer
Server	DSLAM	Firewall 
Telephone	Switch	Router

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

This product is recyclable. Dispose of it properly.



Contents Overview

Introduction **37**

Getting to Know Your ZyWALL 39
Introducing the Web Configurator 43
Wizard Setup 61
Tutorial 81
Registration 101

Network **105**

LAN Screens 107
Bridge Screens 119
WAN Screens 125

Security **139**

Firewall 141
Intrusion Detection and Prevention (IDP) 171
Configuring IDP 175
Anti-Virus 191
IPSec VPN 203
Certificates 243
Authentication Server 271

Advanced **275**

Network Address Translation (NAT) 277
Static Route 293
Remote Management 297
UPnP 319
Custom Application 329
ALG Screen 331

Reports, Logs and Maintenance **337**

Reports 339
Logs 351
Maintenance 375

Zero Configuration **403**

Zero Configuration Screens 405

Troubleshooting and Specifications 417

Troubleshooting 419
Product Specifications 427

Appendices and Index 431

Table of Contents

About This User's Guide **3**

Document Conventions **4**

Safety Warnings **6**

Contents Overview **9**

Table of Contents **11**

List of Figures **23**

List of Tables **31**

Part I: Introduction **37**

Chapter 1
Getting to Know Your ZyWALL **39**

1.1 Overview 39
1.1.1 Secure Network Access for Telecommuters 39
1.1.2 LAN Network Protection 40
1.2 ZyWALL Hardware Connections 40
1.3 LEDs 40

Chapter 2
Introducing the Web Configurator **43**

2.1 Web Configurator Overview 43
2.2 Accessing the ZyWALL Web Configurator 43
2.3 Web Configurator Overview 45
2.3.1 Title Bar 46
2.3.2 Main Window 46
2.3.3 Navigation Panel 46
2.3.4 HOME Screen: Router Mode 50
2.3.5 HOME Screen: Bridge Mode 53
2.3.6 Network Status: More 56
2.3.7 Port Statistics 57
2.3.8 DHCP Table Screen 57
2.3.9 VPN Status 58

Chapter 3
Wizard Setup 61

3.1 Wizard Setup Overview 61
3.2 Internet Access 61
3.2.1 ISP Parameters 62
3.2.2 Internet Access Wizard: Second Screen 66
3.2.3 Internet Access Wizard: Wizard Finish 66
3.2.4 Internet Access Wizard: Registration 67
3.2.5 Internet Access Wizard: Service Activation 70
3.2.6 Internet Access Wizard: Status 71
3.3 VPN Wizard Gateway Setting 71
3.4 VPN Wizard Network Setting 72
3.5 VPN Wizard IKE Tunnel Setting (IKE Phase 1) 74
3.6 VPN Wizard IPSec Setting (IKE Phase 2) 76
3.7 VPN Wizard Status Summary 77
3.8 VPN Wizard Setup Complete 79

Chapter 4
Tutorial 81

4.1 Dynamic VPN Rule Configuration 81
4.1.1 Configure Bob's User Account 82
4.1.2 VPN Gateway and Network Policy Configuration 83
4.1.3 Configure Zero Configuration Mode on ZyWALL B 88
4.1.4 Testing Your VPN Configuration 89
4.2 Security Settings for VPN Traffic 91
4.2.1 IDP for From VPN Traffic Example 91
4.2.2 IDP for To VPN Traffic Example 92
4.3 Firewall Rule for VPN Example 93
4.3.1 Configuring the VPN Rule 94
4.3.2 Configuring the Firewall Rules 98

Chapter 5
Registration 101

5.1 myZyXEL.com overview 101
5.1.1 Subscription Services Available on the ZyWALL 101
5.2 Registration 102
5.3 Service 104

Part II: Network 105

Chapter 6
LAN Screens 107

6.1 LAN, WAN and the ZyWALL 107
6.2 DHCP 108
6.2.1 IP Pool Setup 108
6.3 RIP Setup 108
6.4 Multicast 108
6.5 WINS 109
6.6 DNS Overview 109
6.7 DNS Servers 109
6.7.1 Private DNS Server Behind a Remote IPSec Router 110
6.8 LAN 110
6.9 LAN Static DHCP 113
6.10 LAN IP Alias 114
6.11 MAC Filter 116

Chapter 7
Bridge Screens 119

7.1 Bridge Loop 119
7.2 Spanning Tree Protocol (STP) 120
7.2.1 Rapid STP (RSTP) 120
7.2.2 STP Terminology 120
7.2.3 How STP Works 121
7.2.4 STP Port States 121
7.3 Bridge 121

Chapter 8
WAN Screens 125

8.1 WAN Overview 125
8.2 WAN Route 125
8.3 WAN IP Address Assignment 126
8.4 DNS Server Address Assignment 127
8.5 WAN MAC Address 127
8.6 WAN 127
8.6.1 WAN Ethernet Encapsulation 127
8.6.2 PPPoE Encapsulation 130
8.6.3 PPTP Encapsulation 133
8.7 Dynamic DNS 136
8.7.1 DYNDNS Wildcard 137
8.8 Configuring Dynamic DNS 137

Part III: Security 139

Chapter 9
Firewall 141

9.1 Firewall Overview 141
9.2 Packet Direction Matrix 142
9.3 Packet Direction Examples 143
9.3.1 To VPN Packet Direction 144
9.3.2 From VPN Packet Direction 145
9.3.3 From VPN To VPN Packet Direction 146
9.4 Security Considerations 148
9.5 Firewall Rules Example 148
9.6 Asymmetrical Routes 150
9.6.1 Asymmetrical Routes and IP Alias 150
9.7 Firewall Default Rule (Router Mode) 151
9.8 Firewall Default Rule (Bridge Mode) 153
9.9 Firewall Rule Summary 155
9.9.1 Firewall Edit Rule 157
9.10 Anti-Probing 160
9.11 Firewall Thresholds 161
9.11.1 Threshold Values 162
9.12 Threshold Screen 162
9.13 Service 164
9.13.1 Firewall Edit Custom Service 165
9.14 My Service Firewall Rule Example 165

Chapter 10
Intrusion Detection and Prevention (IDP) 171

10.1 Introduction to IDP 171
10.2 Firewalls and Intrusions 171
10.3 IDS and IDP 172
10.4 Host IDP 172
10.5 Network IDP 172
10.6 Example Intrusions 172
10.6.1 SQL Slammer Worm 173
10.6.2 Blaster W32.Worm 173
10.6.3 Nimda 173
10.6.4 MyDoom 173
10.7 ZyWALL IDP 174

Chapter 11
Configuring IDP 175

11.1 Overview 175
11.2 General Setup 175
11.3 IDP Signatures 177

11.3.1 Attack Types 177
11.3.2 Intrusion Severity 178
11.3.3 Signature Actions 178
11.3.4 Configuring IDP Signatures 179
11.3.5 Query View 181
11.4 Anomaly 185
11.5 Update 187
11.5.1 mySecurityZone 187
11.5.2 Configuring IDP Update 188
11.6 Backup and Restore 189

Chapter 12
Anti-Virus 191

12.1 Anti-Virus Overview 191
12.1.1 Types of Computer Viruses 191
12.1.2 Computer Virus Infection and Prevention 191
12.1.3 Types of Anti-Virus Scanner 192
12.2 Introduction to the ZyWALL Anti-Virus Scanner 192
12.2.1 How the ZyWALL Anti-Virus Scanner Works 192
12.2.2 Notes About the ZyWALL Anti-Virus 193
12.3 General Anti-Virus Setup 193
12.4 Signature Searching 195
12.4.1 Signature Search Example 197
12.5 Signature Update 199
12.5.1 mySecurityZone 199
12.5.2 Configuring Anti-virus Update 199
12.6 Backup and Restore 201

Chapter 13
IPSec VPN 203

13.1 IPSec VPN Overview 203
13.1.1 IKE SA Overview 204
13.2 VPN Rules (IKE) 205
13.3 IKE SA Setup 207
13.3.1 IKE SA Proposal 207
13.4 Additional IPSec VPN Topics 212
13.4.1 Dynamic IPSec Rule 212
13.4.2 Full Feature NAT Mode 212
13.4.3 SA Life Time 212
13.4.4 IPSec High Availability 213
13.4.5 Encryption and Authentication Algorithms 214
13.5 VPN Rules (IKE) Gateway Policy Edit 214
13.6 IPSec SA Overview 220

13.6.1 Local and Remote Networks 221
13.6.2 Virtual Address Mapping 221
13.6.3 Active Protocol 223
13.6.4 Encapsulation 223
13.6.5 IPSec SA Proposal and Perfect Forward Secrecy 224
13.7 Network Policy Edit 225
13.8 Network Policy Port Forwarding 230
13.9 Network Policy Move 232
13.10 Dialing the VPN Tunnel via Web Configurator 233
13.11 IPSec Debug 234
13.12 VPN SA Monitor 235
13.13 VPN Global Setting 236
13.13.1 Local and Remote IP Address Conflict Resolution 236
13.14 Telecommuter VPN/IPSec Examples 239
13.14.1 Telecommuters Sharing One VPN Rule Example 240
13.14.2 Telecommuters Using Unique VPN Rules Example 240
13.15 VPN and Remote Management 242

Chapter 14
Certificates 243

14.1 Certificates Overview 243
14.1.1 Advantages of Certificates 244
14.2 Self-signed Certificates 244
14.3 Verifying a Certificate 244
14.3.1 Checking the Fingerprint of a Certificate on Your Computer 244
14.4 Configuration Summary 245
14.5 My Certificates 246
14.6 My Certificate Details 247
14.7 My Certificate Export 250
14.7.1 Certificate File Export Formats 250
14.8 My Certificate Import 251
14.8.1 Certificate File Formats 251
14.9 My Certificate Create 253
14.10 Trusted CAs 256
14.11 Trusted CA Details 258
14.12 Trusted CA Import 261
14.13 Trusted Remote Hosts 262
14.14 Trusted Remote Hosts Import 264
14.15 Trusted Remote Host Certificate Details 265
14.16 Directory Servers 267
14.17 Directory Server Add or Edit 268

Chapter 15
Authentication Server 271

15.1 Authentication Server Overview 271
15.1.1 Local User Database 271
15.1.2 RADIUS 271
15.2 Local User Database 272
15.3 RADIUS 273

Part IV: Advanced 275

Chapter 16
Network Address Translation (NAT) 277

16.1 NAT Overview 277
16.1.1 NAT Definitions 277
16.1.2 What NAT Does 278
16.1.3 How NAT Works 278
16.1.4 NAT Application 279
16.1.5 Port Restricted Cone NAT 279
16.1.6 NAT Mapping Types 280
16.2 Using NAT 281
16.2.1 SUA (Single User Account) Versus NAT 281
16.3 NAT Overview Screen 281
16.4 NAT Address Mapping 283
16.4.1 What NAT Does 283
16.4.2 NAT Address Mapping Edit 285
16.5 Port Forwarding 286
16.5.1 Default Server IP Address 286
16.5.2 Port Forwarding: Services and Port Numbers 287
16.5.3 Configuring Servers Behind Port Forwarding (Example) 287
16.5.4 Port Translation 287
16.6 Port Forwarding Screen 288
16.7 Port Triggering 290

Chapter 17
Static Route 293

17.1 IP Static Route 293
17.2 IP Static Route 293
17.2.1 IP Static Route Edit 294

Chapter 18
Remote Management 297

18.1 Remote Management Overview 297
18.1.1 Remote Management Limitations 298

18.1.2 System Timeout 298
18.2 WWW (HTTP and HTTPS) 298
18.3 WWW Configuration 299
18.4 HTTPS Example 301
18.4.1 Internet Explorer Warning Messages 301
18.4.2 Netscape Navigator Warning Messages 301
18.4.3 Avoiding the Browser Warning Messages 302
18.4.4 Login Screen 303
18.5 SSH 305
18.6 How SSH Works 305
18.7 SSH Implementation on the ZyWALL 306
18.7.1 Requirements for Using SSH 306
18.8 Configuring SSH 307
18.9 Secure Telnet Using SSH Examples 308
18.9.1 Example 1: Microsoft Windows 308
18.9.2 Example 2: Linux 308
18.10 Secure FTP Using SSH Example 309
18.11 Telnet 310
18.12 Configuring TELNET 310
18.13 Telnet Login 311
18.14 FTP 311
18.15 SNMP 312
18.15.1 Supported MIBs 313
18.15.2 SNMP Traps 314
18.15.3 REMOTE MANAGEMENT: SNMP 314
18.16 DNS 315
18.17 Introducing Vantage CNM 316
18.18 Configuring CNM 316
18.18.1 Additional Configuration for Vantage CNM 318

Chapter 19
UPnP 319

19.1 Universal Plug and Play Overview 319
19.1.1 How Do I Know If I'm Using UPnP? 319
19.1.2 NAT Traversal 319
19.1.3 Cautions with UPnP 319
19.1.4 UPnP and ZyXEL 320
19.2 Configuring UPnP 320
19.3 Displaying UPnP Port Mapping 321
19.4 Installing UPnP in Windows Example 322
19.4.1 Installing UPnP in Windows Me 323
19.4.2 Installing UPnP in Windows XP 324
19.5 Using UPnP in Windows XP Example 324

19.5.1 Auto-discover Your UPnP-enabled Network Device 325
19.5.2 Web Configurator Easy Access 326

Chapter 20
Custom Application 329

20.1 Custom Applicaton 329
20.2 Custom Applicaton Configuration 329

Chapter 21
ALG Screen 331

21.1 ALG Introduction 331
21.1.1 ALG and NAT 331
21.1.2 ALG and the Firewall 331
21.2 FTP 332
21.3 H.323 332
21.4 RTP 332
21.4.1 H.323 ALG Details 332
21.5 SIP 334
21.5.1 STUN 334
21.5.2 SIP ALG Details 334
21.5.3 SIP Signaling Session Timeout 334
21.5.4 SIP Audio Session Timeout 335
21.6 ALG Screen 335

Part V: Reports, Logs and Maintenance 337

Chapter 22
Reports 339

22.1 Configuring Reports 339
22.2 Traffic Statistics Screen 339
22.2.1 Viewing Web Site Hits 341
22.2.2 Viewing Host IP Address 341
22.2.3 Viewing Protocol/Port 342
22.2.4 System Reports Specifications 343
22.3 IDP Screen 344
22.4 Anti-Virus Screen 346
22.5 E-mail Report Screen 347

Chapter 23
Logs 351

23.1 View Log 351

23.2 Log Description Example 352
23.2.1 About the Certificate Not Trusted Log 352
23.3 Configuring Log Settings 353
23.3.1 Log Descriptions 357
23.4 Syslog Logs 373

Chapter 24
Maintenance 375

24.1 Maintenance Overview 375
24.2 General Setup and System Name 375
24.3 General Setup 375
24.4 Configuring Password 377
24.5 Brute-Force Password Guessing Protection 378
24.6 Time and Date 378
24.7 Pre-defined NTP Time Server Pools 381
24.7.1 Resetting the Time 381
24.7.2 Time Server Synchronization 381
24.8 Introduction To Transparent Bridging 382
24.9 Transparent Firewalls 383
24.10 Configuring Device Mode (Router) 383
24.11 Configuring Device Mode (Bridge) 385
24.12 Configuring Device Mode (Zero Configuration) 386
24.12.1 Network Conflict Avoidance 387
24.13 Configuring Device Mode (Zero Configuration) 387
24.14 Firmware and Configuration File Maintenance 388
24.15 Filename Conventions 389
24.16 File Maintenance Over WAN 389
24.17 F/W Upload Screen 390
24.18 Backup and Restore 391
24.18.1 Backup Configuration 392
24.18.2 Restore Configuration 392
24.18.3 Back to Factory Defaults 393
24.19 Using FTP or TFTP to Back Up Configuration 394
24.19.1 Using the FTP Commands to Back Up Configuration 394
24.19.2 FTP Command Configuration Backup Example 394
24.19.3 Configuration Backup Using GUI-based FTP Clients 395
24.19.4 Backup Configuration Using TFTP 395
24.19.5 TFTP Command Configuration Backup Example 395
24.19.6 Configuration Backup Using GUI-based TFTP Clients 396
24.20 Using FTP or TFTP to Restore Configuration 396
24.20.1 Restore Using FTP Session Example 397
24.21 FTP and TFTP Firmware and Configuration File Uploads 397
24.21.1 FTP File Upload Command from the DOS Prompt Example 397

24.21.2 FTP Session Example of Firmware File Upload 398
24.21.3 TFTP File Upload 398
24.21.4 TFTP Upload Command Example 398
24.22 Restart Screen 399
24.23 Diagnostics 399

Part VI: Zero Configuration 403

Chapter 25
Zero Configuration Screens 405

25.1 Overview 405
25.1.1 What You Can Do in the Zero Configuration Screens 406
25.2 The Internet Access Screen 406
25.2.1 Network Status 406
25.2.2 ISP Parameters 407
25.3 The VPN Screen 412
25.3.1 VPN Activation 412
25.3.2 The SA Monitor Screen 413
25.4 The Security Screen 414
25.5 The Logs Screen 415

Part VII: Troubleshooting and Specifications 417

Chapter 26
Troubleshooting 419

26.1 Power, Hardware Connections, and LEDs 419
26.2 ZyWALL Access and Login 420
26.3 Internet Access 422
26.4 VoIP 424
26.5 Advanced Features 424
26.6 Resetting the ZyWALL to Its Factory Defaults 425
26.7 Packet Flow 425

Chapter 27
Product Specifications 427

27.1 Specification Tables 427
27.2 Cable Pin Assignments 430
27.3 Power Specifications 430

Part VIII: Appendices and Index 431

Appendix A Setting up Your Computer's IP Address 433

Appendix B Pop-up Windows, JavaScripts and Java Permissions 449

Appendix C IP Addresses and Subnetting 455

Appendix D Common Services 463

Appendix E Windows 98 SE/Me Requirements for Anti-Virus Message Display 467

Appendix F Importing Certificates 471

Appendix G Command Interpreter 481

Appendix H NetBIOS Filter Commands 487

Appendix I Legal Information 489

Appendix J Customer Support 493

Index 499

List of Figures

Figure 1 Application: Telecommuters 39
Figure 2 Application: LAN Network Protection 40
Figure 3 Front Panel: LEDs 41
Figure 4 Web Configurator: Login Screen 44
Figure 5 Change Password Screen 44
Figure 6 Replace Certificate Screen 45
Figure 7 HOME Screen 45
Figure 8 Web Configurator HOME Screen in Router Mode 50
Figure 9 Web Configurator HOME Screen in Bridge Mode 54
Figure 10 HOME > more 56
Figure 11 HOME > Show Statistics 57
Figure 12 HOME > DHCP Table 58
Figure 13 HOME > VPN Status 59
Figure 14 Wizard Setup Welcome 61
Figure 15 ISP Parameters: Ethernet Encapsulation 62
Figure 16 ISP Parameters: PPPoE Encapsulation 63
Figure 17 ISP Parameters: PPTP Encapsulation 65
Figure 18 Internet Access Wizard: Second Screen 66
Figure 19 Internet Access Setup Complete 67
Figure 20 Internet Access Wizard: Registration 68
Figure 21 Internet Access Wizard: Registered Device 68
Figure 22 Internet Access Wizard: Registration in Progress 69
Figure 23 Internet Access Wizard: Registration Failed 69
Figure 24 Service Activation 70
Figure 25 Internet Access Wizard: Activated Services 70
Figure 26 Internet Access Wizard: Registration in Progress 71
Figure 27 Internet Access Wizard: Status 71
Figure 28 VPN Wizard: Gateway Setting 72
Figure 29 VPN Wizard: Network Setting 73
Figure 30 VPN Wizard: IKE Tunnel Setting 74
Figure 31 VPN Wizard: IPSec Setting 76
Figure 32 VPN Wizard: VPN Status 78
Figure 33 VPN Wizard Setup Complete 80
Figure 34 Dynamic VPN Rule Example 81
Figure 35 VPN Gateway Policy Edit Screens 84
Figure 36 SECURITY > VPN > Add Network Policy (ZyWALL A) 85
Figure 37 VPN Network Policy Edit Screens 86
Figure 38 Activate VPN Rule (ZyWALL B) 87

Figure 39 VPN Summary Screens 88
Figure 40 Check The Telecommuter's Computer IP Address 89
Figure 41 Telecommuter Pinging a Network X IP Address Example 90
Figure 42 Tutorial: IDP for From VPN Traffic 91
Figure 43 Tutorial: IDP Configuration for Traffic From VPN 92
Figure 44 Tutorial: IDP for To VPN Traffic 92
Figure 45 Tutorial: IDP Configuration for To VPN Traffic 93
Figure 46 Tutorial: Firewall Rule for VPN 93
Figure 47 Tutorial: SECURITY > VPN > VPN Rules (IKE) 94
Figure 48 Tutorial: SECURITY > VPN > VPN Rules (IKE)> Add Gateway Policy 95
Figure 49 Tutorial: SECURITY > VPN > VPN Rules (IKE): With Gateway Policy Example 96
Figure 50 Tutorial: SECURITY > VPN > VPN Rules (IKE)> Add Network Policy 97
Figure 51 Tutorial: SECURITY > FIREWALL > Rule Summary 98
Figure 52 Tutorial: SECURITY > FIREWALL > Rule Summary > Edit: Allow 99
Figure 53 Tutorial: SECURITY > FIREWALL > Rule Summary: Allow 100
Figure 54 Tutorial: SECURITY > FIREWALL > Default Rule: Block From VPN To LAN 100
Figure 55 REGISTRATION 102
Figure 56 REGISTRATION: Registered Device 103
Figure 57 REGISTRATION > Service 104
Figure 58 LAN and WAN 107
Figure 59 Private DNS Server Example 110
Figure 60 NETWORK > LAN 111
Figure 61 NETWORK > LAN > Static DHCP 114
Figure 62 Physical Network and Partitioned Logical Networks 115
Figure 63 NETWORK > LAN > IP Alias 115
Figure 64 NETWORK > LAN > MAC Address Filter 117
Figure 65 Bridge Loop: Bridge Connected to Wired LAN 119
Figure 66 NETWORK > Bridge 122
Figure 67 NETWORK > WAN (Route) 125
Figure 68 NETWORK > WAN > WAN (Ethernet Encapsulation) 128
Figure 69 NETWORK > WAN > WAN (PPPoE Encapsulation) 131
Figure 70 NETWORK > WAN > WAN (PPTP Encapsulation) 134
Figure 71 NETWORK > WAN > DDNS 137
Figure 72 Default Firewall Action 141
Figure 73 SECURITY > FIREWALL > Default Rule (Router Mode) 142
Figure 74 Default Block Traffic From WAN to LAN Example 143
Figure 75 From LAN to VPN Example 145
Figure 76 Block LAN to VPN Traffic by Default Example 145
Figure 77 From VPN to LAN Example 146
Figure 78 Block VPN to LAN Traffic by Default Example 146
Figure 79 From VPN to VPN Example 147
Figure 80 Block VPN to VPN Traffic by Default Example 147
Figure 81 Blocking All LAN to WAN IRC Traffic Example 148

Figure 82 Limited LAN to WAN IRC Traffic Example 149
Figure 83 Using IP Alias to Solve the Triangle Route Problem 151
Figure 84 SECURITY > FIREWALL > Default Rule (Router Mode) 151
Figure 85 SECURITY > FIREWALL > Default Rule (Bridge Mode) 154
Figure 86 SECURITY > FIREWALL > Rule Summary 156
Figure 87 SECURITY > FIREWALL > Rule Summary > Edit 158
Figure 88 SECURITY > FIREWALL > Anti-Probing 160
Figure 89 Three-Way Handshake 161
Figure 90 SECURITY > FIREWALL > Threshold 162
Figure 91 SECURITY > FIREWALL > Service 164
Figure 92 Firewall Edit Custom Service 165
Figure 93 My Service Firewall Rule Example: Service 166
Figure 94 My Service Firewall Rule Example: Edit Custom Service 166
Figure 95 My Service Firewall Rule Example: Rule Summary 166
Figure 96 My Service Firewall Rule Example: Rule Edit 167
Figure 97 My Service Firewall Rule Example: Rule Configuration 168
Figure 98 My Service Firewall Rule Example: Rule Summary 169
Figure 99 Network Intrusions 171
Figure 100 Applying IDP to Interfaces 175
Figure 101 SECURITY > IDP > General 176
Figure 102 SECURITY > IDP > Signatures: Attack Types 177
Figure 103 SECURITY > IDP > Signature: Actions 179
Figure 104 SECURITY > IDP > Signature: Group View 179
Figure 105 SECURITY > IDP > Signature: Query View 181
Figure 106 SECURITY > IDP > Signature: Query by Partial Name 184
Figure 107 SECURITY > IDP > Signature: Query by Complete ID 184
Figure 108 Signature Query by Attribute. 185
Figure 109 SECURITY > IDP > Anomaly 186
Figure 110 SECURITY > IDP > Update 188
Figure 111 SECURITY > IDP > Backup & Restore 190
Figure 112 ZyWALL Anti-virus Example 193
Figure 113 SECURITY > ANTI-VIRUS > General 194
Figure 114 SECURITY > ANTI-VIRUS > Signature: Query View 196
Figure 115 Query Example Search Criteria 197
Figure 116 Query Example Search Results 198
Figure 117 SECURITY > ANTI-VIRUS > Update 200
Figure 118 SECURITY > ANTI-VIRUS > Backup and Restore 201
Figure 119 VPN: Example 203
Figure 120 VPN: IKE SA and IPSec SA 204
Figure 121 Gateway and Network Policies 205
Figure 122 IPSec Fields Summary 205
Figure 123 SECURITY > VPN > VPN Rules (IKE) 206
Figure 124 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal 208

Figure 125 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange 208
Figure 126 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication 209
Figure 127 VPN/NAT Example 211
Figure 128 IPSec High Availability 213
Figure 129 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy 215
Figure 130 Virtual Mapping of Local and Remote Network IP Addresses 222
Figure 131 Virtual Mapping of Local and Remote Network IP Addresses 223
Figure 132 VPN: Transport and Tunnel Mode Encapsulation 224
Figure 133 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy 226
Figure 134 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy > Port Forwarding 231
Figure 135 SECURITY > VPN > VPN Rules (IKE) > Move Network Policy 232
Figure 136 VPN Rule Configured 233
Figure 137 VPN Dial 233
Figure 138 VPN Tunnel Established 233
Figure 139 IKE/IPSec Debug Example 235
Figure 140 SECURITY > VPN > SA Monitor 236
Figure 141 Overlap in a Dynamic VPN Rule 237
Figure 142 Overlap in IP Alias and VPN Remote Networks 238
Figure 143 SECURITY > VPN > Global Setting 238
Figure 144 Telecommuters Sharing One VPN Rule Example 240
Figure 145 Telecommuters Using Unique VPN Rules Example 241
Figure 146 VPN for Remote Management Example 242
Figure 147 Certificates on Your Computer 244
Figure 148 Certificate Details 245
Figure 149 Certificate Configuration Overview 245
Figure 150 SECURITY > CERTIFICATES > My Certificates 246
Figure 151 SECURITY > CERTIFICATES > My Certificates > Details 248
Figure 152 SECURITY > CERTIFICATES > My Certificates > Export 251
Figure 153 SECURITY > CERTIFICATES > My Certificates > Import 252
Figure 154 SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12 253
Figure 155 SECURITY > CERTIFICATES > My Certificates > Create 254
Figure 156 SECURITY > CERTIFICATES > Trusted CAs 257
Figure 157 SECURITY > CERTIFICATES > Trusted CAs > Details 259
Figure 158 SECURITY > CERTIFICATES > Trusted CAs > Import 262
Figure 159 SECURITY > CERTIFICATES > Trusted Remote Hosts 263
Figure 160 SECURITY > CERTIFICATES > Trusted Remote Hosts > Import 264
Figure 161 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details 265
Figure 162 SECURITY > CERTIFICATES > Directory Servers 267
Figure 163 SECURITY > CERTIFICATES > Directory Server > Add 268
Figure 164 SECURITY > AUTH SERVER > Local User Database 272
Figure 165 SECURITY > AUTH SERVER > RADIUS 273
Figure 166 How NAT Works 278
Figure 167 NAT Application With IP Alias 279

Figure 168 Port Restricted Cone NAT Example 280
Figure 169 ADVANCED > NAT > NAT Overview 282
Figure 170 ADVANCED > NAT > Address Mapping 284
Figure 171 ADVANCED > NAT > Address Mapping > Edit 285
Figure 172 Multiple Servers Behind NAT Example 287
Figure 173 Port Translation Example 288
Figure 174 ADVANCED > NAT > Port Forwarding 289
Figure 175 Trigger Port Forwarding Process: Example 290
Figure 176 ADVANCED > NAT > Port Triggering 291
Figure 177 Example of Static Routing Topology 293
Figure 178 ADVANCED > STATIC ROUTE > IP Static Route 294
Figure 179 ADVANCED > STATIC ROUTE > IP Static Route > Edit 295
Figure 180 Secure and Insecure Remote Management From the WAN 297
Figure 181 HTTPS Implementation 299
Figure 182 ADVANCED > REMOTE MGMT > WWW 300
Figure 183 Security Alert Dialog Box (Internet Explorer) 301
Figure 184 Security Certificate 1 (Netscape) 302
Figure 185 Security Certificate 2 (Netscape) 302
Figure 186 Example: Lock Denoting a Secure Connection) 303
Figure 187 Replace Certificate 304
Figure 188 Device-specific Certificate 304
Figure 189 Common ZyWALL Certificate 305
Figure 190 SSH Communication Over the WAN Example 305
Figure 191 How SSH Works 306
Figure 192 ADVANCED > REMOTE MGMT > SSH 307
Figure 193 SSH Example 1: Store Host Key 308
Figure 194 SSH Example 2: Test 308
Figure 195 SSH Example 2: Log in 309
Figure 196 Secure FTP: Firmware Upload Example 309
Figure 197 ADVANCED > REMOTE MGMT > Telnet 310
Figure 198 ADVANCED > REMOTE MGMT > FTP 311
Figure 199 SNMP Management Model 313
Figure 200 ADVANCED > REMOTE MGMT > SNMP 314
Figure 201 ADVANCED > REMOTE MGMT > DNS 316
Figure 202 ADVANCED > REMOTE MGMT > CNM 317
Figure 203 ADVANCED > UPnP 320
Figure 204 ADVANCED > UPnP > Ports 321
Figure 205 ADVANCED > Custom APP 330
Figure 206 H.323 ALG Example 332
Figure 207 H.323 with Multiple WAN IP Addresses 333
Figure 208 H.323 Calls from the WAN with Multiple Outgoing Calls 333
Figure 209 SIP ALG Example 334
Figure 210 ADVANCED > ALG 335

Figure 211 REPORTS > Traffic Statistics 340
Figure 212 REPORTS > Traffic Statistics: Web Site Hits Example 341
Figure 213 REPORTS > Traffic Statistics: Host IP Address Example 342
Figure 214 REPORTS > Traffic Statistics: Protocol/Port Example 343
Figure 215 REPORTS > IDP 344
Figure 216 REPORTS > IDP > Source 345
Figure 217 REPORTS > IDP > Destination 346
Figure 218 REPORTS > Anti-Virus 346
Figure 219 REPORTS > Anti-Virus > Source 347
Figure 220 REPORTS > Anti-Virus > Destination 347
Figure 221 REPORTS > E-mail Report 348
Figure 222 LOGS > View Log 351
Figure 223 myZyXEL.com: Download Center 353
Figure 224 myZyXEL.com: Certificate Download 353
Figure 225 LOGS > Log Settings 355
Figure 226 MAINTENANCE > General Setup 376
Figure 227 MAINTENANCE > Password 377
Figure 228 MAINTENANCE > Time and Date 379
Figure 229 Synchronization in Process 381
Figure 230 Synchronization is Successful 382
Figure 231 Synchronization Fail 382
Figure 232 MAINTENANCE > Device Mode (Router Mode) 384
Figure 233 MAINTENANCE > Device Mode (Bridge Mode) 385
Figure 234 MAINTENANCE > Device Mode (Zero Configuration Mode) 387
Figure 235 MAINTENANCE > Firmware Upload 390
Figure 236 Firmware Upload In Process 391
Figure 237 Network Temporarily Disconnected 391
Figure 238 Firmware Upload Error 391
Figure 239 MAINTENANCE > Backup and Restore 392
Figure 240 Configuration Upload Successful 393
Figure 241 Network Temporarily Disconnected 393
Figure 242 Configuration Upload Error 393
Figure 243 Reset Warning Message 394
Figure 244 FTP Session Example 394
Figure 245 Restore Using FTP Session Example 397
Figure 246 FTP Session Example of Firmware File Upload 398
Figure 247 MAINTENANCE > Restart 399
Figure 248 MAINTENANCE > Diagnostics 400
Figure 249 Zero Configuration 405
Figure 250 INTERNET ACCESS (Network Status) 406
Figure 251 INTERNET ACCESS (Ethernet Encapsulation) 408
Figure 252 INTERNET ACCESS (PPPoE Encapsulation) 409
Figure 253 INTERNET ACCESS (PPTP Encapsulation) 411

Figure 254 VPN 413
Figure 255 VPN 413
Figure 256 SA Monitor 414
Figure 257 SECURITY 414
Figure 258 LOGS 415
Figure 259 WIndows 95/98/Me: Network: Configuration 434
Figure 260 Windows 95/98/Me: TCP/IP Properties: IP Address 435
Figure 261 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 436
Figure 262 Windows XP: Start Menu 437
Figure 263 Windows XP: Control Panel 437
Figure 264 Windows XP: Control Panel: Network Connections: Properties 438
Figure 265 Windows XP: Local Area Connection Properties 438
Figure 266 Windows XP: Internet Protocol (TCP/IP) Properties 439
Figure 267 Windows XP: Advanced TCP/IP Properties 440
Figure 268 Windows XP: Internet Protocol (TCP/IP) Properties 441
Figure 269 Macintosh OS 8/9: Apple Menu 442
Figure 270 Macintosh OS 8/9: TCP/IP 442
Figure 271 Macintosh OS X: Apple Menu 443
Figure 272 Macintosh OS X: Network 444
Figure 273 Red Hat 9.0: KDE: Network Configuration: Devices 445
Figure 274 Red Hat 9.0: KDE: Ethernet Device: General 445
Figure 275 Red Hat 9.0: KDE: Network Configuration: DNS 446
Figure 276 Red Hat 9.0: KDE: Network Configuration: Activate 446
Figure 277 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 447
Figure 278 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 447
Figure 279 Red Hat 9.0: DNS Settings in resolv.conf 447
Figure 280 Red Hat 9.0: Restart Ethernet Card 447
Figure 281 Red Hat 9.0: Checking TCP/IP Properties 448
Figure 282 Pop-up Blocker 449
Figure 283 Internet Options: Privacy 450
Figure 284 Internet Options: Privacy 451
Figure 285 Pop-up Blocker Settings 451
Figure 286 Internet Options: Security 452
Figure 287 Security Settings - Java Scripting 453
Figure 288 Security Settings - Java 453
Figure 289 Java (Sun) 454
Figure 290 Network Number and Host ID 456
Figure 291 Subnetting Example: Before Subnetting 458
Figure 292 Subnetting Example: After Subnetting 459
Figure 293 Windows 98 SE: WinPopup 467
Figure 294 WIndows 98 SE: Program Task Bar 468
Figure 295 Windows 98 SE: Task Bar Properties 468
Figure 296 Windows 98 SE: StartUp 469

Figure 297 Windows 98 SE: Startup: Create Shortcut 469
Figure 298 Windows 98 SE: Startup: Select a Title for the Program 470
Figure 299 Windows 98 SE: Startup: Shortcut 470
Figure 300 Security Certificate 471
Figure 301 Login Screen 472
Figure 302 Certificate General Information before Import 472
Figure 303 Certificate Import Wizard 1 473
Figure 304 Certificate Import Wizard 2 473
Figure 305 Certificate Import Wizard 3 474
Figure 306 Root Certificate Store 474
Figure 307 Certificate General Information after Import 475
Figure 308 ZyWALL Trusted CA Screen 476
Figure 309 CA Certificate Example 477
Figure 310 Personal Certificate Import Wizard 1 477
Figure 311 Personal Certificate Import Wizard 2 478
Figure 312 Personal Certificate Import Wizard 3 478
Figure 313 Personal Certificate Import Wizard 4 479
Figure 314 Personal Certificate Import Wizard 5 479
Figure 315 Personal Certificate Import Wizard 6 479
Figure 316 Access the ZyWALL Via HTTPS 480
Figure 317 SSL Client Authentication 480
Figure 318 ZyWALL Secure Login Screen 480
Figure 319 Displaying Log Categories Example 482
Figure 320 Displaying Log Parameters Example 482
Figure 321 Routing Command Example 483
Figure 322 Backup Gateway 485
Figure 323 Routing Command Example 486

List of Tables

Table 1 LED Descriptions 41
Table 2 Title Bar: Web Configurator Icons 46
Table 3 Device Mode Features Comparison 46
Table 4 Screens Summary 47
Table 5 Web Configurator HOME Screen in Router Mode 50
Table 6 Web Configurator HOME Screen in Bridge Mode 54
Table 7 HOME > more 56
Table 8 HOME > Show Statistics 57
Table 9 HOME > DHCP Table 58
Table 10 HOME > VPN Status 59
Table 11 ISP Parameters: Ethernet Encapsulation 62
Table 12 ISP Parameters: PPPoE Encapsulation 64
Table 13 ISP Parameters: PPTP Encapsulation 65
Table 14 Internet Access Wizard: Registration 68
Table 15 Service Activation 70
Table 16 VPN Wizard: Gateway Setting 72
Table 17 VPN Wizard: Network Setting 73
Table 18 VPN Wizard: IKE Tunnel Setting 75
Table 19 VPN Wizard: IPSec Setting 76
Table 20 VPN Wizard: VPN Status 78
Table 21 Dynamic VPN Rule Tutorial Settings 82
Table 22 REGISTRATION 103
Table 23 REGISTRATION > Service 104
Table 24 NETWORK > LAN 111
Table 25 NETWORK > LAN > Static DHCP 114
Table 26 NETWORK > LAN > IP Alias 115
Table 27 NETWORK > LAN > MAC Address Filter 117
Table 28 STP Path Costs 120
Table 29 STP Port States 121
Table 30 NETWORK > Bridge 122
Table 31 NETWORK > WAN (Route) 126
Table 32 Private IP Address Ranges 126
Table 33 NETWORK > WAN > WAN (Ethernet Encapsulation) 128
Table 34 NETWORK > WAN > WAN (PPPoE Encapsulation) 131
Table 35 NETWORK > WAN > WAN (PPTP Encapsulation) 134
Table 36 NETWORK > WAN > DDNS 138
Table 37 Blocking All LAN to WAN IRC Traffic Example 149
Table 38 Limited LAN to WAN IRC Traffic Example 149

Table 39 SECURITY > FIREWALL > Default Rule (Router Mode) 152
Table 40 SECURITY > FIREWALL > Default Rule (Bridge Mode) 154
Table 41 SECURITY > FIREWALL > Rule Summary 156
Table 42 SECURITY > FIREWALL > Rule Summary > Edit 159
Table 43 SECURITY > FIREWALL > Anti-Probing 161
Table 44 SECURITY > FIREWALL > Threshold 163
Table 45 SECURITY > FIREWALL > Service 164
Table 46 SECURITY > FIREWALL > Service > Add 165
Table 47 SECURITY > IDP > General Setup 176
Table 48 SECURITY > IDP > Signature: Attack Types 177
Table 49 SECURITY > IDP > Signature: Intrusion Severity 178
Table 50 SECURITY > IDP > Signature: Actions 179
Table 51 SECURITY > IDP > Signature: Group View 180
Table 52 SECURITY > IDP > Signature: Query View 181
Table 53 SECURITY > IDP > Anomaly 186
Table 54 SECURITY > IDP > Update 188
Table 55 Common Computer Virus Types 191
Table 56 SECURITY > ANTI-VIRUS > General 194
Table 57 SECURITY > ANTI-VIRUS > Signature: Query View 196
Table 58 SECURITY > ANTI-VIRUS > Update 200
Table 59 SECURITY > VPN > VPN Rules (IKE) 206
Table 60 VPN Example: Matching ID Type and Content 209
Table 61 VPN Example: Mismatching ID Type and Content 210
Table 62 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy 216
Table 63 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy 227
Table 64 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy > Port Forwarding 231
Table 65 SECURITY > VPN > VPN Rules (IKE) > Move Network Policy 232
Table 66 SECURITY > VPN > SA Monitor 236
Table 67 SECURITY > VPN > Global Setting 238
Table 68 Telecommuters Sharing One VPN Rule Example 240
Table 69 Telecommuters Using Unique VPN Rules Example 241
Table 70 SECURITY > CERTIFICATES > My Certificates 246
Table 71 SECURITY > CERTIFICATES > My Certificates > Details 248
Table 72 SECURITY > CERTIFICATES > My Certificates > Export 251
Table 73 SECURITY > CERTIFICATES > My Certificates > Import 252
Table 74 SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12 253
Table 75 SECURITY > CERTIFICATES > My Certificates > Create 254
Table 76 SECURITY > CERTIFICATES > Trusted CAs 257
Table 77 SECURITY > CERTIFICATES > Trusted CAs > Details 259
Table 78 SECURITY > CERTIFICATES > Trusted CAs Import 262
Table 79 SECURITY > CERTIFICATES > Trusted Remote Hosts 263
Table 80 SECURITY > CERTIFICATES > Trusted Remote Hosts > Import 264
Table 81 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details 266

Table 82 SECURITY > CERTIFICATES > Directory Servers 268
Table 83 SECURITY > CERTIFICATES > Directory Server > Add 269
Table 84 SECURITY > AUTH SERVER > Local User Database 273
Table 85 SECURITY > AUTH SERVER > RADIUS 273
Table 86 NAT Definitions 277
Table 87 NAT Mapping Types 280
Table 88 ADVANCED > NAT > NAT Overview 282
Table 89 ADVANCED > NAT > Address Mapping 284
Table 90 ADVANCED > NAT > Address Mapping > Edit 286
Table 91 ADVANCED > NAT > Port Forwarding 289
Table 92 ADVANCED > NAT > Port Triggering 291
Table 93 ADVANCED > STATIC ROUTE > IP Static Route 294
Table 94 ADVANCED > STATIC ROUTE > IP Static Route > Edit 295
Table 95 ADVANCED > REMOTE MGMT > WWW 300
Table 96 ADVANCED > REMOTE MGMT > SSH 307
Table 97 ADVANCED > REMOTE MGMT > Telnet 310
Table 98 ADVANCED > REMOTE MGMT > FTP 312
Table 99 SNMP Traps 314
Table 100 ADVANCED > REMOTE MGMT > SNMP 315
Table 101 ADVANCED > REMOTE MGMT > DNS 316
Table 102 ADVANCED > REMOTE MGMT > CNM 317
Table 103 ADVANCED > UPnP 320
Table 104 ADVANCED > UPnP > Ports 321
Table 105 ADVANCED > Custom APP 330
Table 106 ADVANCED > ALG 335
Table 107 REPORTS > Traffic Statistics 340
Table 108 REPORTS > Traffic Statistics: Web Site Hits Report 341
Table 109 REPORTS > Traffic Statistics: Host IP Address 342
Table 110 REPORTS > Traffic Statistics: Protocol/ Port 343
Table 111 Report Specifications 343
Table 112 REPORTS > IDP 344
Table 113 REPORTS > Anti-Virus 346
Table 114 REPORTS > E-mail Report 348
Table 115 LOGS > View Log 351
Table 116 Log Description Example 352
Table 117 LOGS > Log Settings 356
Table 118 System Maintenance Logs 357
Table 119 System Error Logs 358
Table 120 Access Control Logs 359
Table 121 TCP Reset Logs 359
Table 122 Packet Filter Logs 360
Table 123 ICMP Logs 360
Table 124 CDR Logs 361

Table 125 PPP Logs 361
Table 126 UPnP Logs 361
Table 127 Attack Logs 361
Table 128 Remote Management Logs 363
Table 129 MAC Filter Logs 363
Table 130 IPSec Logs 363
Table 131 IKE Logs 364
Table 132 PKI Logs 367
Table 133 Certificate Path Verification Failure Reason Codes 368
Table 134 802.1X Logs 369
Table 135 ACL Setting Notes 369
Table 136 ICMP Notes 370
Table 137 IDP Logs 371
Table 138 AV Logs 371
Table 139 Syslog Logs 373
Table 140 RFC-2408 ISAKMP Payload Types 374
Table 141 MAINTENANCE > General Setup 376
Table 142 MAINTENANCE > Password 377
Table 143 Brute-Force Password Guessing Protection Commands 378
Table 144 MAINTENANCE > Time and Date 379
Table 145 MAC-address-to-port Mapping Table 382
Table 146 MAINTENANCE > Device Mode (Router Mode) 384
Table 147 MAINTENANCE > Device Mode (Bridge Mode) 385
Table 148 MAINTENANCE > Device Mode (Zero Configuration Mode) 387
Table 149 Filename Conventions 389
Table 150 MAINTENANCE > Firmware Upload 390
Table 151 Restore Configuration 392
Table 152 General Commands for GUI-based FTP Clients 395
Table 153 General Commands for GUI-based TFTP Clients 396
Table 154 MAINTENANCE > Diagnostics 400
Table 155 INTERNET ACCESS (Network Status) 407
Table 156 INTERNET ACCESS (Ethernet Encapsulation) 408
Table 157 INTERNET ACCESS (PPPoE Encapsulation) 409
Table 158 INTERNET ACCESS (PPTP Encapsulation) 411
Table 159 VPN Activation 413
Table 160 SA Monitor 414
Table 161 SECURITY 415
Table 162 LOGS 416
Table 163 Hardware Specifications 427
Table 164 Firmware Specifications 427
Table 165 Feature and Performance Specifications 429
Table 166 Ethernet Cable Pin Assignments 430
Table 167 AC Power Adaptor Specifications 430

Table 168 IP Address Network Number and Host ID Example 456
Table 169 Subnet Masks 457
Table 170 Maximum Host Numbers 457
Table 171 Alternative Subnet Mask Notation 457
Table 172 Subnet 1 459
Table 173 Subnet 2 460
Table 174 Subnet 3 460
Table 175 Subnet 4 460
Table 176 Eight Subnets 460
Table 177 24-bit Network Number Subnet Planning 461
Table 178 16-bit Network Number Subnet Planning 461
Table 179 Commonly Used Services 463
Table 180 NetBIOS Filter Default Settings 487

PART I
Introduction

Getting to Know Your ZyWALL (39)
Introducing the Web Configurator (43)
Wizard Setup (61)
Tutorial (81)
Registration (101)

1

Getting to Know Your ZyWALL

This chapter introduces the main features and applications of the ZyWALL.

1.1 Overview

The ZyWALL can be pre-configured by a network administrator to make it a plug-and-play security device for mobile telecommuters who need a secure connection to the company network through the Internet

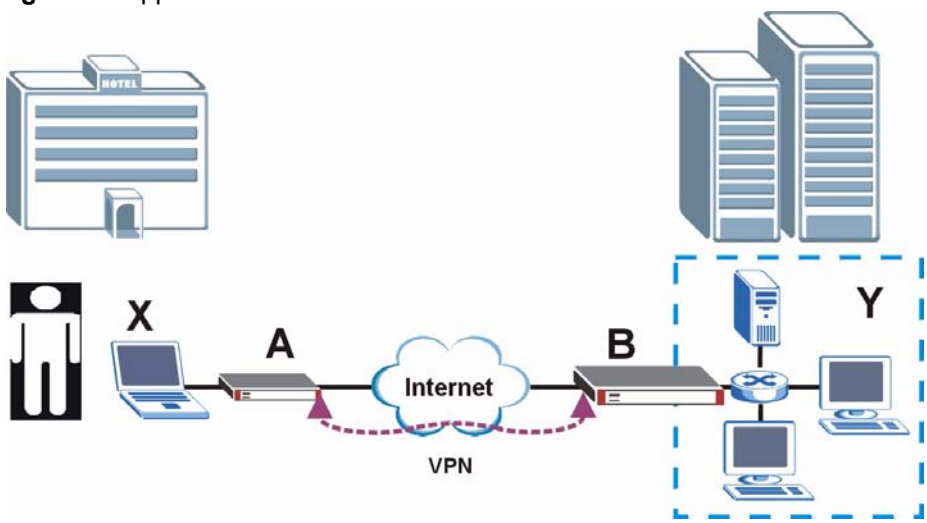
By integrating NAT, firewall, Intrusion Detection and Prevention (IDP), anti-virus scanning, certificates and VPN capability, the ZyWALL is a complete security solution that protects your computer. In addition, the embedded web configurator is easy to operate.

You can also deploy the ZyWALL as a transparent firewall in an existing network with minimal configuration.

1.1.1 Secure Network Access for Telecommuters

The following figure shows a VPN network example. A telecommuter can simply connect the pre-configured ZyWALL and enter the VPN account information to establish a VPN connection through the Internet to headquarters.

Figure 1 Application: Telecommuters

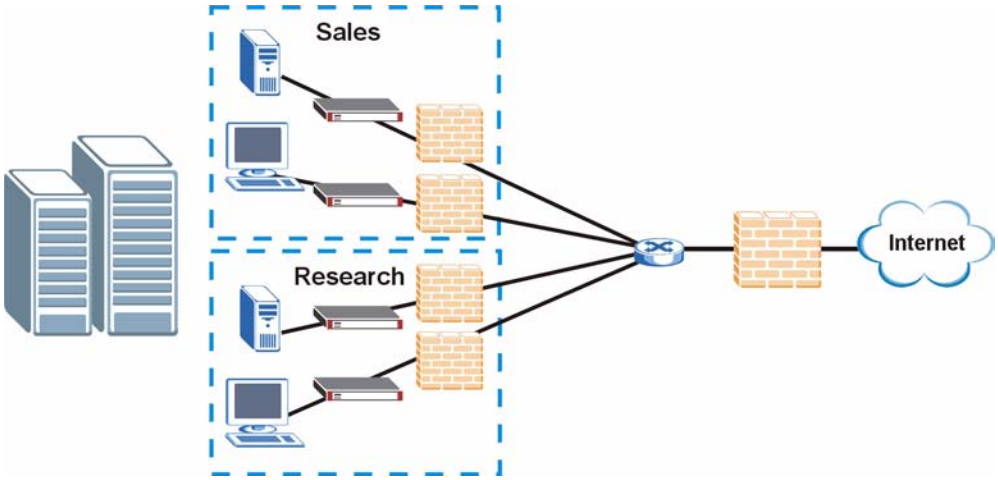


1.1.2 LAN Network Protection

In most cases, firewalls are deployed to protect the local network (LAN) from attacks originating from the WAN (such as the Internet). However, security outbreaks are possible on the LAN via other means (such as file sharing with removable storage devices). You can use the ZyWALL to provide network security on the LAN.

In the following example, computers in the Sales and Research departments are protected from each other by the ZyWALLs on the LAN.

Figure 2 Application: LAN Network Protection



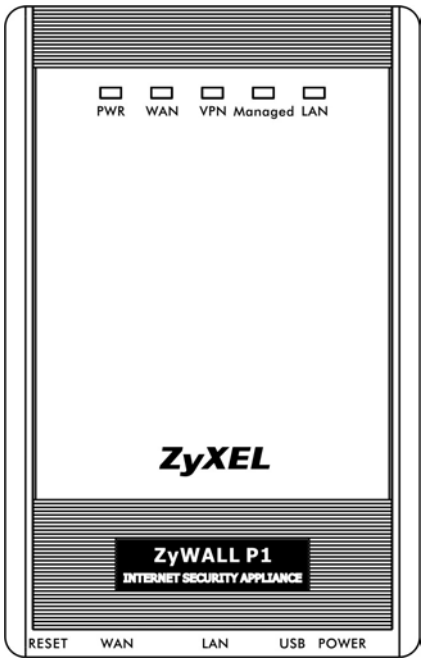
1.2 ZyWALL Hardware Connections

Refer to the Quick Start Guide for information on hardware connection and basic setup.

1.3 LEDs

The following figure shows the LEDs.

Figure 3 Front Panel: LEDs



The following table describes the LEDs.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR		Off	The ZyWALL is turned off.
	Green	On	The ZyWALL is turned on.
		Blinking	The ZyWALL is starting.
WAN		Off	The WAN connection is not ready, or has failed.
	Green	On	The ZyWALL has a successful 10Mbps WAN connection.
		Blinking	The 10M WAN is sending or receiving packets.
	Amber	On	The ZyWALL has a successful 100Mbps WAN connection.
		Blinking	The 100M WAN is sending or receiving packets.
VPN		Off	The ZyWALL does not have a VON connection.
	Green	On	The ZyWALL has a successful VPN connection.
		Blinking	The ZyWALL is receiving or sending data through the VPN connection.
Managed		Off	The ZyWALL does not have a CNM connection.
	Green	On	The ZyWALL has a successful CNM connection.
		Blinking	The ZyWALL is receiving or sending data using CNM.
LAN		Off	The LAN is not connected.
	Green	On	The ZyWALL has a successful 10Mbps LAN connection.
		Blinking	The 10M LAN is sending or receiving packets.
	Amber	On	The ZyWALL has a successful 100Mbps LAN connection.
		Blinking	The 100M LAN is sending or receiving packets.

2

Introducing the Web Configurator

This chapter describes how to access the ZyWALL web configurator and provides an overview of its screens.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy ZyWALL setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See Appendix B on page 449 if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

2.2 Accessing the ZyWALL Web Configurator

Use the following process to log into the web configurator when the ZyWALL is in router or bridge mode. See Chapter 25 on page 405 for how to access the web configurator with zero configuration mode.

1. Make sure your ZyWALL hardware is properly connected and prepare your computer/ computer network to connect to the ZyWALL (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type the ZyWALL's IP address as the URL ("192.168.167.1" is the default). Alternatively, if you have enabled the management FQDN (Fully Qualified Domain Name), you can use the management domain name to access the ZyWALL from the LAN (see Section 24.3 on page 375 for details).
4. A login screen displays. Type the password ("1234" is the default) and click **Login**. In some versions, the default password appears automatically - if this is the case, click

Login. If you forget your password or cannot access the web configurator, you will need to use the ZyWALL's physical **RESET** button. See

Figure 4 Web Configurator: Login Screen

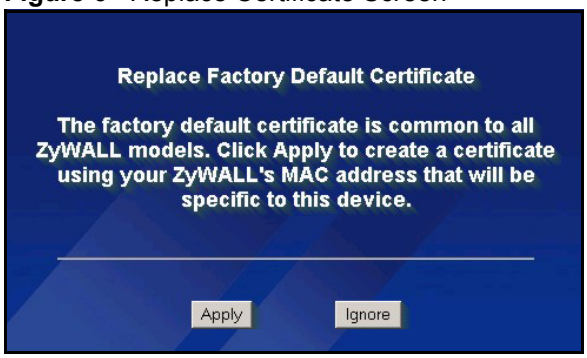
5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 5 Change Password Screen

6 Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyWALL's MAC address that will be specific to this device.

If you do not replace the default certificate here or in the **CERTIFICATES** screen, this screen displays every time you access the web configurator.

Figure 6 Replace Certificate Screen


Replace Factory Default Certificate
The factory default certificate is common to all ZyWALL models. Click Apply to create a certificate using your ZyWALL's MAC address that will be specific to this device.
Apply
Ignore

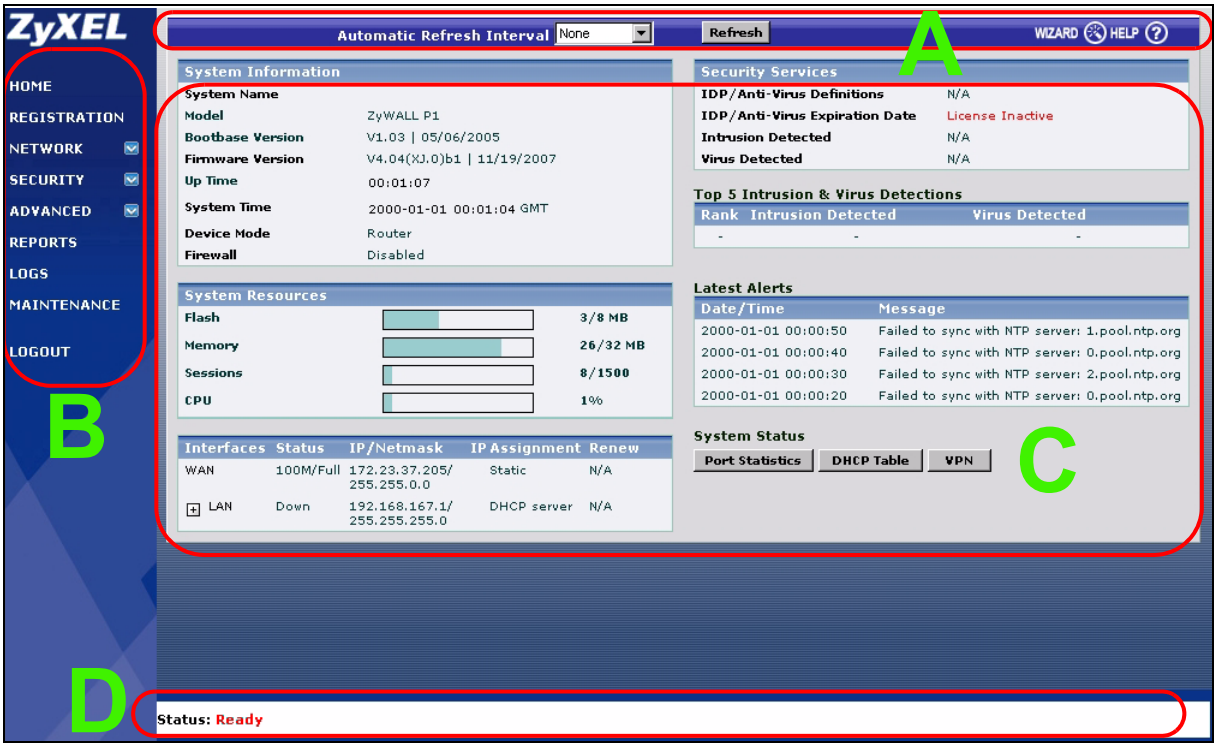
7 You should now see the **HOME** screen (see Figure 7 on page 45).

The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the ZyWALL if this happens to you.

2.3 Web Configurator Overview

The following sections introduce the layout and navigation of the web configurator screens.

Figure 7 HOME Screen



As illustrated above, the web configurator screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

2.3.1 Title Bar

The title bar provides some icons in the upper right corner. The icons provide the following functions.

Table 2 Title Bar: Web Configurator Icons

ICON	DESCRIPTION
	Wizards: Click this icon to open one of the web configurator wizards. See Chapter 3 on page 61 for more information.
	Help: Click this icon to open the help page for the current screen.

2.3.2 Main Window

The main window shows the screen you select in the navigation panel. It is discussed in more detail in the rest of this document.

Right after you log in, the **HOME** screen displays. The screen varies according to the device mode you select in the **MAINTENANCE > Device Mode** screen.

2.3.3 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure ZyWALL features.

The following table lists the features available for each device mode.

Table 3 Device Mode Features Comparison

FEATURE	ROUTER MODE	ZERO CONFIGURATION MODE	BRIDGE MODE
Internet Access Wizard	O	O	
VPN Wizard	O	O	O
DHCP Table	O	O	
System Statistics	O	O	O
Registration	O	O	O
LAN	O	O	
LAN IP Alias	O		
LAN MAC Filter		O	
WAN	O	O	
Bridge			O
Firewall	O	O	O
IDP	O	O	O
Anti-Virus	O	O	O

Table 3 Device Mode Features Comparison

FEATURE	ROUTER MODE	ZERO CONFIGURATION MODE	BRIDGE MODE
VPN	O	O	O
Certificates	O	O	O
Authentication Server	O	O	O
NAT	O	O	
NAT Address Mapping	O		
Static Route	O	O	
Remote Management	O	O	O
UPnP	O	O	
Custom Application	O	O	O
ALG	O	O	O
Logs	O	O	O
Maintenance	O	O	O

Table Key: An O in a mode's column shows that the device mode has the specified feature. The information in this table was correct at the time of writing, although it may be subject to change.

The following table describes the sub-menus.

Table 4 Screens Summary

LINK	TAB	FUNCTION
HOME		This screen shows the ZyWALL's general device and network status information. Use this screen to access the wizards, statistics and DHCP table.
REGISTRATION	Registration	Use this screen to register your ZyWALL and activate the trial service subscriptions.
	Service	Use this to manage and update the service status and license information.
NETWORK		
LAN	LAN	Use this screen to configure LAN DHCP and TCP/IP settings.
	Static DHCP	Use this screen to assign fixed IP addresses on the LAN.
	IP Alias	Use this screen to partition your LAN interface into subnets.
	MAC Filter	Use this screen to specify the MAC addresses of computers that can access the ZyWALL.
BRIDGE	Bridge	Use this screen to change the bridge settings on the ZyWALL.
WAN	Route	This screen allows you to configure route priority.
	WAN	Use this screen to configure the WAN port for internet access.
	DDNS	Use this screen to set up dynamic DNS.
SECURITY		

Table 4 Screens Summary (continued)

LINK	TAB	FUNCTION
FIREWALL	Default Rule	Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule
	Rule Summary	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti-Probing	Use this screen to change your anti-probing settings.
	Threshold	Use this screen to configure the threshold for DoS attacks.
	Service	Use this screen to configure custom services.
IDP	General	Use this screen to enable IDP on the ZyWALL and choose what interface(s) you want to protect from intrusions.
	Signature	Use these screens to view signatures by attack type or search for signatures by signature name, ID, severity, target operating system, action etc. You can also configure signature actions here.
	Anomaly	Use this screen to configure your ADP (Anomaly Detection and Prevention) settings.
	Update	Use this screen to download new signature downloads. It is important to do this as new intrusions evolve.
	Backup & Restore	Use this screen to back up, restore or revert to the default signatures' actions.
ANTI-VIRUS	General	Use this screen to activate AV scanning on the interface(s) and specify actions when a virus is detected.
	Signature	Use these screens to search for signatures by signature name or attributes and configure how the ZyWALL uses them.
	Update	Use this screen to view the version number of the current signatures and configure the signature update schedule.
	Backup & Restore	Use this screen to back up, restore or revert to the default signatures' actions.
VPN	VPN Rules (IKE)	Use this screen to configure VPN connections using IKE key management and view the rule summary.
	SA Monitor	Use this screen to display and manage active VPN connections.
	Global Setting	Use this screen to configure the IPSec timer settings.
CERTIFICATES	My Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CAs	Use this screen to view and manage the list of the trusted CAs.
	Trusted Remote Hosts	Use this screen to view and manage the certificates belonging to the trusted remote hosts.
	Directory Servers	Use this screen to view and manage the list of the directory servers.
AUTH SERVER	Local User Database	Use this screen to configure the local user account(s) on the ZyWALL to authenticate VPN users.
	RADIUS	Configure this screen to use an external server to authenticate VPN users.
ADVANCED		

Table 4 Screens Summary (continued)

LINK	TAB	FUNCTION
NAT	NAT Overview	Use this screen to enable NAT.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	Port Forwarding	Use this screen to configure servers behind the ZyWALL.
	Port Triggering	Use this screen to change your ZyWALL's port triggering settings.
STATIC ROUTE	IP Static Route	Use this screen to configure IP static routes.
REMOTE MGMT	WWW	Use this screen to configure through which interfaces and from which IP address(es) users can use HTTPS or HTTP to manage the ZyWALL.
	SSH	Use this screen to configure through which interfaces and from which IP address(es) users can use Secure Shell to manage the ZyWALL.
	TELNET	Use this screen to configure through which interfaces and from which IP address(es) users can use Telnet to manage the ZyWALL.
	FTP	Use this screen to configure through which interfaces and from which IP address(es) users can use FTP to access the ZyWALL.
	SNMP	Use this screen to configure your ZyWALL's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interfaces and from which IP address(es) users can send DNS queries to the ZyWALL.
	CNM	Use this screen to configure and allow your ZyWALL to be managed by the Vantage CNM server.
UPnP	UPnP	Use this screen to enable UPnP on the ZyWALL.
	Ports	Use this screen to view the NAT port mapping rules that UPnP creates on the ZyWALL.
Custom APP	Custom APP	Use this screen to specify port numbers for the ZyWALL to monitor for FTP, HTTP, SMTP, POP3, H323, and SIP traffic.
ALG	ALG	Use this screen to allow certain applications to pass through the ZyWALL.
REPORTS	Traffic Statistics	Use this screen to have the ZyWALL record and display network usage reports.
	IDP	Use this screen to collect and display statistics on the intrusions that the ZyWALL has detected.
	Anti-Virus	Use this screen to collect and display statistics on the viruses that the ZyWALL has detected.
	E-Mail Report	Use this screen to configure the settings for sending reports via email.
LOGS	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your ZyWALL's log settings.

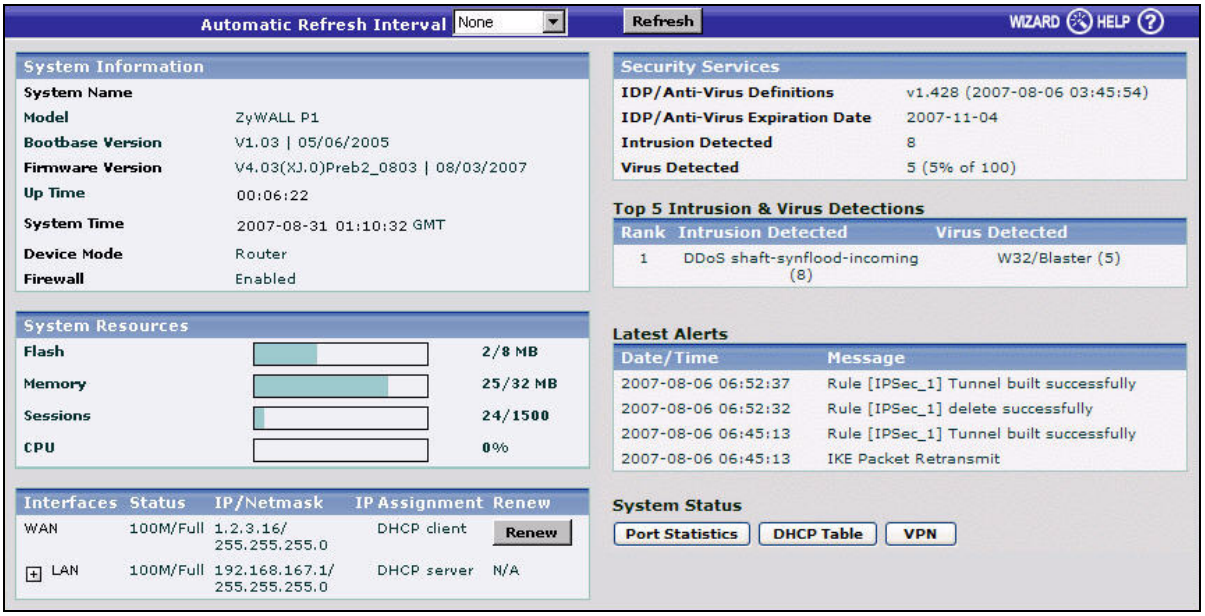
Table 4 Screens Summary (continued)

LINK	TAB	FUNCTION
MAINTENANCE	General	This screen contains administrative settings, including the IP system DNS server IP addresses.
	Password	Use this screen to change your password.
	Time and Date	Use this screen to change your ZyWALL's time and date.
	Device Mode	Use this screen to configure and have your ZyWALL work as a router or a bridge.
	F/W Upload	Use this screen to upload firmware to your ZyWALL
	Backup & Restore	Use this screen to backup and restore the configuration or reset the factory defaults to your ZyWALL.
	Restart	This screen allows you to reboot the ZyWALL without turning the power off.
	Diagnostic	Use this screen to have the ZyWALL generate and send diagnostic information by e-mail and/or the console port.
LOGOUT		Click this label to exit the web configurator.

2.3.4 HOME Screen: Router Mode

The following screen displays when the ZyWALL is set to router mode. This screen displays general status information about the ZyWALL. The ZyWALL is set to router mode by default.

Figure 8 Web Configurator HOME Screen in Router Mode



The following table describes the labels in this screen.

Table 5 Web Configurator HOME Screen in Router Mode

LABEL	DESCRIPTION
Automatic Refresh Interval	Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh	Click this button to update the status screen statistics immediately.

Table 5 Web Configurator HOME Screen in Router Mode (continued)

LABEL	DESCRIPTION
System Information	
System Name	This is the **System Name** you enter in the **MAINTENANCE > General** screen. It is for identification purposes. Click the field label to go to the screen where you can specify a name for this ZyWALL.
Model	This is the model name of your ZyWALL.
Bootbase Version	This is the bootbase version and the date created.
Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design. Click the field label to go to the screen where you can upload a new firmware file.
Up Time	This field displays how long the ZyWALL has been running since it last started up. The ZyWALL starts up when you turn it on, when you restart it (**MAINTENANCE > Restart**), or when you reset it (see Section 26.6 on page 425).
System Time	This field displays your ZyWALL's present date (in yyyy-mm-dd format) and time (in hh:mm:ss format) along with the difference from the Greenwich Mean Time (GMT) zone. The difference from GMT is based on the time zone. It is also adjusted for Daylight Saving Time if you set the ZyWALL to use it. Click the field label to go to the screen where you can modify the ZyWALL's date and time settings.
Device Mode	This displays whether the ZyWALL is functioning as a router, bridge or simplified router (zero configuration mode). Click the field label to go to the screen where you can configure the device mode.
Firewall	This displays whether or not the ZyWALL's firewall is activated. Click the field label to go to the screen where you can turn the firewall on or off.
System Resources	
Flash	The first number shows how many megabytes of the flash the ZyWALL is using.
Memory	The first number shows how many megabytes of the heap memory the ZyWALL is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT, VPN and the firewall. The second number shows the ZyWALL's total heap memory (in megabytes). The bar displays what percent of the ZyWALL's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Sessions	The first number shows how many sessions are currently open on the ZyWALL. This includes all sessions that are currently traversing the ZyWALL, terminating at the ZyWALL or Initiated from the ZyWALL The second number is the maximum number of sessions that can be open at one time. The bar displays what percent of the maximum number of sessions is in use. The bar turns from green to red when the maximum is being approached.
CPU	This field displays what percentage of the ZyWALL's processing ability is currently used. When this percentage is close to 100%, the ZyWALL is running at full load, and the throughput is not going to increase anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using the firewall.
Interfaces	This is the port type. Click "+" to expand or "-" to collapse the IP alias drop-down lists. Hold your cursor over an interface's label to display the interface's MAC Address. Click an interface's label to go to the screen where you can configure settings for that interface.

Table 5 Web Configurator HOME Screen in Router Mode (continued)

LABEL	DESCRIPTION
Status	For the LAN port, this displays the port speed and duplex setting. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect. For the WAN port the port speed and duplex setting display if you're using Ethernet encapsulation and **Down** (line is down or not connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you're using PPPoE encapsulation.
IP/Netmask	This shows the port's IP address and subnet mask.
IP Assignment	For the WAN, if the ZyWALL gets its IP address automatically from an ISP, this displays **DHCP client** when you're using Ethernet encapsulation and **IPCP Client** when you're using PPPoE or PPTP encapsulation. **Static** displays if the WAN port is using a manually entered static (fixed) IP address. For the LAN, **DHCP server** displays when the ZyWALL is set to automatically give IP address information to the computers connected to the LAN. **DHCP relay** displays when the ZyWALL is set to forward IP address assignment requests to another DHCP server. Static displays if the LAN port is using a manually entered static (fixed) IP address. In this case, you must have another DHCP server on your LAN, or else the computers must be manually configured.
Renew	If you are using Ethernet encapsulation and the WAN port is configured to get the IP address automatically from the ISP, click **Renew** to release the WAN port's dynamically assigned IP address and get the IP address afresh. Click **Dial** to dial up the PPTP or PPPoE connection. Click **Drop** to disconnect the PPTP or PPPoE connection.
Security Services	
IDP/Anti-Virus Definitions	This is the version number of the signatures set that the ZyWALL is using and the date and time that the set was released. Click the field label to go to the screen where you can update the signatures. N/A displays when the service subscription has expired.
IDP/Anti-Virus Expiration Date	This is the date the IDP/anti-virus service subscription expires. Click the field label to go to the screen where you can update your service subscription.
Intrusion Detected	This displays how many intrusions the ZyWALL has detected since it last started up. N/A displays when the ZyWALL has never had an IDP subscription. Disable displays when IDP threat statistics collection is disabled. Click the field label to go to the related screen.
Virus Detected	This displays how many virus-infected files the ZyWALL has detected since it last started up. It also displays the percentage of virus-infected files out of the total number of files that the ZyWALL has scanned (since it last started up). N/A displays when the ZyWALL has never had an anti-virus subscription. Disable displays when anti-virus threat statistics collection is disabled. Click the field label to go to the related screen.
Top 5 Intrusion & Virus Detections	The following is a list of the five intrusions or viruses that the ZyWALL has most frequently detected since it last started up.
Rank	This is the ranking number of an intrusion or virus. This is an intrusion's or virus's place in the list of most common intrusions or viruses.
Intrusion Detected	This is the name of a signature for which the ZyWALL has detected matching packets. The number in brackets indicates how many times the signature has been matched.
Virus Detected	This is the name of the virus that the ZyWALL has detected.

Table 5 Web Configurator HOME Screen in Router Mode (continued)

LABEL	DESCRIPTION
Latest Alerts	This table displays the five most recent alerts recorded by the ZyWALL. You can see more information in the **View Log** screen, such as the source and destination IP addresses and port numbers of the incoming packets.
Date/Time	This is the date and time the alert was recorded.
Message	This is the reason for the alert.
System Status	
Port Statistics	Click **Port Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port.
DHCP Table	Click **DHCP Table** to show current DHCP client information.
VPN	Click **VPN** to display the active VPN connections.

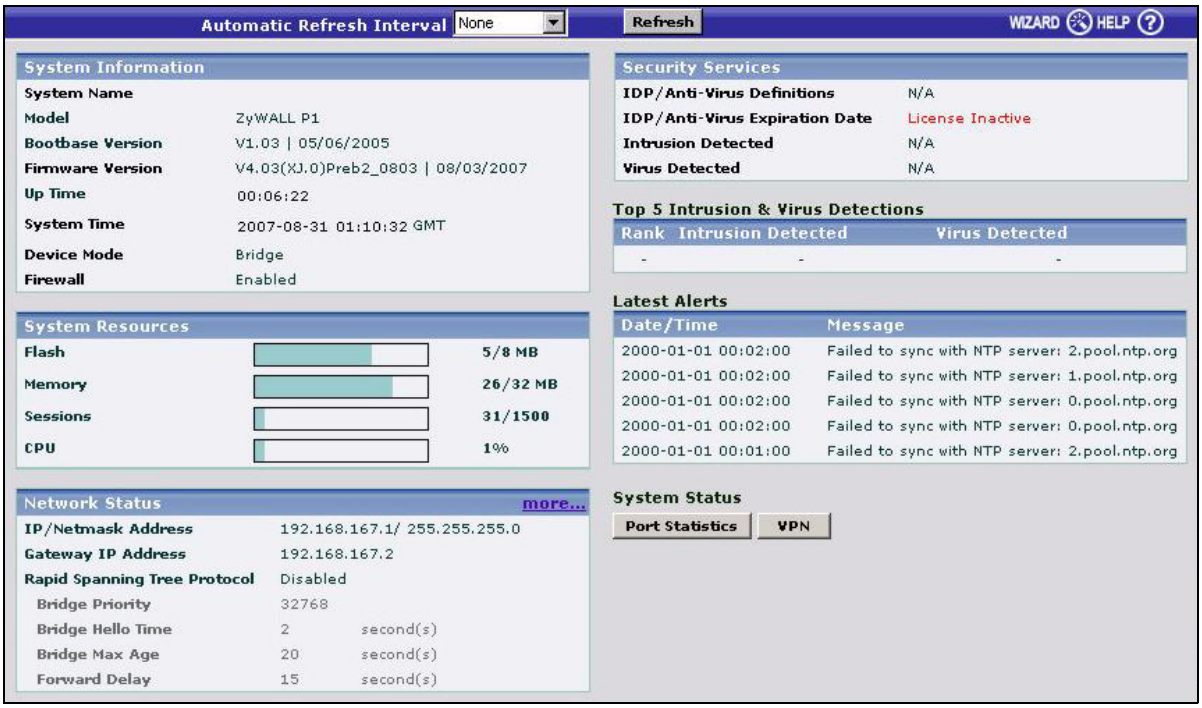
2.3.5 HOME Screen: Bridge Mode

The following screen displays when the ZyWALL is set to bridge mode. In bridge mode, the ZyWALL functions as a transparent firewall (also known as a bridge firewall). The ZyWALL bridges traffic traveling between the ZyWALL's interfaces and still filters and inspects packets. You do not need to change the configuration of your existing network.

In bridge mode, the ZyWALL cannot get an IP address from a DHCP server. The LAN and WAN interfaces have the same (static) IP address and subnet mask. You can configure the ZyWALL's IP address in order to access the ZyWALL for management. If you connect your computer directly to the ZyWALL, you also need to assign your computer a static IP address in the same subnet as the ZyWALL's IP address in order to access the ZyWALL.

You can use the firewall and VPN in bridge mode. See the user’s guide for a list of other features that are available in bridge mode.

Figure 9 Web Configurator HOME Screen in Bridge Mode



The following table describes the labels in this screen.

Table 6 Web Configurator HOME Screen in Bridge Mode

LABEL	DESCRIPTION
Automatic Refresh Interval	Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh	Click this button to update the screen's statistics immediately.
System Information	
System Name	This is the **System Name** you enter in the **MAINTENANCE > General** screen. It is for identification purposes. Click the field label to go to the screen where you can specify a name for this ZyWALL.
Model	This is the model name of your ZyWALL.
Bootbase Version	This is the bootbase version and the date created.
Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design. Click the field label to go to the screen where you can upload a new firmware file.
Up Time	This field displays how long the ZyWALL has been running since it last started up. The ZyWALL starts up when you turn it on, when you restart it (**MAINTENANCE > Restart**), or when you reset it (see Section 26.6 on page 425).
System Time	This field displays your ZyWALL's present date (in yyyy-mm-dd format) and time (in hh:mm:ss format) along with the difference from the Greenwich Mean Time (GMT) zone. The difference from GMT is based on the time zone. It is also adjusted for Daylight Saving Time if you set the ZyWALL to use it. Click the field label to go to the screen where you can modify the ZyWALL's date and time settings.
Device Mode	This displays whether the ZyWALL is functioning as a router, bridge or simplified router (zero configuration mode). Click the field label to go to the screen where you can configure the device mode.

Table 6 Web Configurator HOME Screen in Bridge Mode (continued)

LABEL	DESCRIPTION
Firewall	This displays whether or not the ZyWALL's firewall is activated. Click the field label to go to the screen where you can turn the firewall on or off.
System Resources	
Flash	The first number shows how many megabytes of the flash the ZyWALL is using.
Memory	The first number shows how many megabytes of the heap memory the ZyWALL is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT, VPN and the firewall. The second number shows the ZyWALL's total heap memory (in megabytes). The bar displays what percent of the ZyWALL's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Sessions	The first number shows how many sessions are currently open on the ZyWALL. This includes all sessions that are currently traversing the ZyWALL, terminating at the ZyWALL or initiated from the ZyWALL The second number is the maximum number of sessions that can be open at one time. The bar displays what percent of the maximum number of sessions is in use. The bar turns from green to red when the maximum is being approached.
CPU	This field displays what percentage of the ZyWALL's processing ability is currently used. When this percentage is close to 100%, the ZyWALL is running at full load, and the throughput is not going to increase anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using the firewall.
Network Status	
IP/Netmask Address	This is the IP address and subnet mask of your ZyWALL in dotted decimal notation.
Gateway IP Address	This is the gateway IP address.
Rapid Spanning Tree Protocol	This shows whether RSTP (Rapid Spanning Tree Protocol) is active or not. The following labels or values relative to RSTP do not apply when RSTP is disabled.
Bridge Priority	This is the bridge priority of the ZyWALL. The bridge (or switch) with the lowest bridge priority value in the network is the root bridge (the base of the spanning tree).
Bridge Hello Time	This is the interval of BPDUs (Bridge Protocol Data Units) from the root bridge.
Bridge Max Age	This is the predefined interval that a bridge waits to get a Hello message (BPDU) from the root bridge.
Forward Delay	This is the forward delay interval.
Security Services	
IDP/Anti-Virus Definitions	This is the version number of the signatures set that the ZyWALL is using and the date and time that the set was released. Click the field label to go to the screen where you can update the signatures. N/A displays when the service subscription has expired.
IDP/Anti-Virus Expiration Date	This is the date the IDP/anti-virus service subscription expires. Click the field label to go to the screen where you can update your service subscription.
Intrusion Detected	This displays how many intrusions the ZyWALL has detected since it last started up. N/A displays when the service subscription has expired.

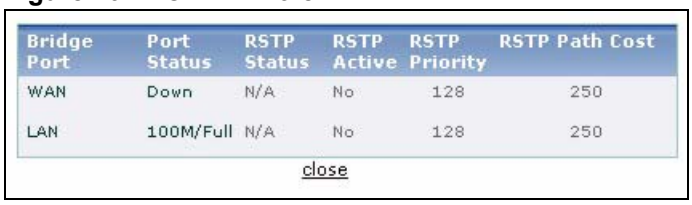
Table 6 Web Configurator HOME Screen in Bridge Mode (continued)

LABEL	DESCRIPTION
Virus Detected	This displays how many virus-infected files the ZyWALL has detected since it last started up. It also displays the percentage of virus-infected files out of the total number of files that the ZyWALL has scanned (since it last started up). N/A displays when the service subscription has expired.
Top 5 Intrusion & Virus Detections	The following is a list of the five intrusions or viruses that the ZyWALL has most frequently detected since it last started up.
Rank	This is the ranking number of an intrusion or virus. This is an intrusion's or virus's place in the list of most common intrusions or viruses.
Intrusion Detected	This is the name of a signature for which the ZyWALL has detected matching packets. The number in brackets indicates how many times the signature has been matched. Click the hyperlink for more detailed information on the intrusion.
Virus Detected	This is the name of the virus that the ZyWALL has detected.
Latest Alerts	This table displays the five most recent alerts recorded by the ZyWALL. You can see more information in the **View Log** screen, such as the source and destination IP addresses and port numbers of the incoming packets.
Date/Time	This is the date and time the alert was recorded.
Message	This is the reason for the alert.
System Status	
Port Statistics	Click **Port Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port.
VPN	Click **VPN** to display the active VPN connections.

2.3.6 Network Status: More

In the **Home** screen, click **more** in the **Network Status** section of the screen to display the following screen of additional RSTP information.

Figure 10 HOME > more



The following table describes the labels in this screen.

Table 7 HOME > more

LABEL	DESCRIPTION
Bridge Port	This is the port type. Port types are: **WAN** and **LAN**.
Port Status	For the WAN and LAN interfaces, this displays the port speed and duplex setting. For the WAN port, it displays **Down** when the link is not ready or has failed.
RSTP Status	This is the RSTP status of the corresponding port.
RSTP Active	This shows whether or not RSTP is active on the corresponding port.
RSTP Priority	This is the RSTP priority of the corresponding port.

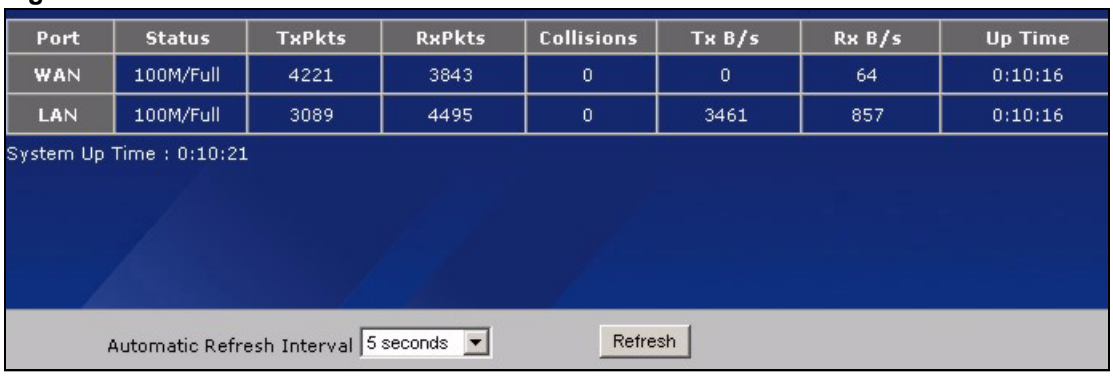
Table 7 HOME > more (continued)

LABEL	DESCRIPTION
RSTP Path Cost	This is the cost of transmitting a frame from the root bridge to the corresponding port.
close	Click this link to collapse this screen.

2.3.7 Port Statistics

Click **Port Statistics** in the **HOME** screen. Read-only information here includes port status and packet specific statistics. The **Poll Interval(s)** field is configurable.

Figure 11 HOME > Show Statistics



The following table describes the labels in this screen.

Table 8 HOME > Show Statistics

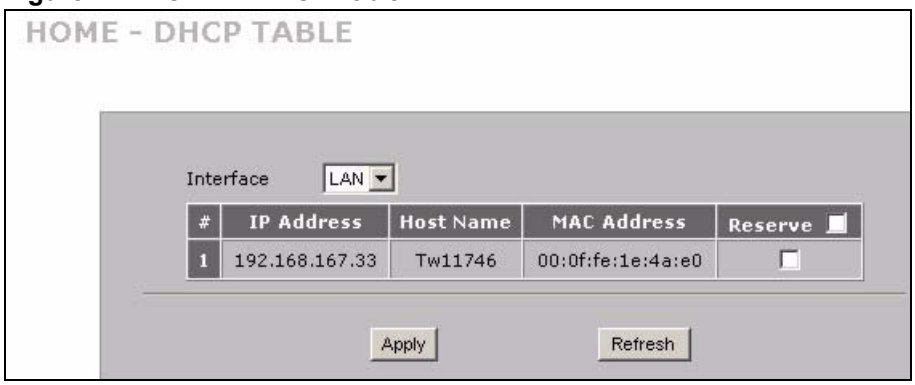
LABEL	DESCRIPTION
Port	These are the ZyWALL's interfaces.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the ZyWALL has been on.
Automatic Refresh Interval	Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh	Click this button to update the screen's statistics immediately.

2.3.8 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyWALL as a DHCP server or disable it. When configured as a server, the ZyWALL provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Show DHCP Table** in the **HOME** screen when the ZyWALL is set to router mode. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the ZyWALL's DHCP server.

Figure 12 HOME > DHCP Table



The following table describes the labels in this screen.

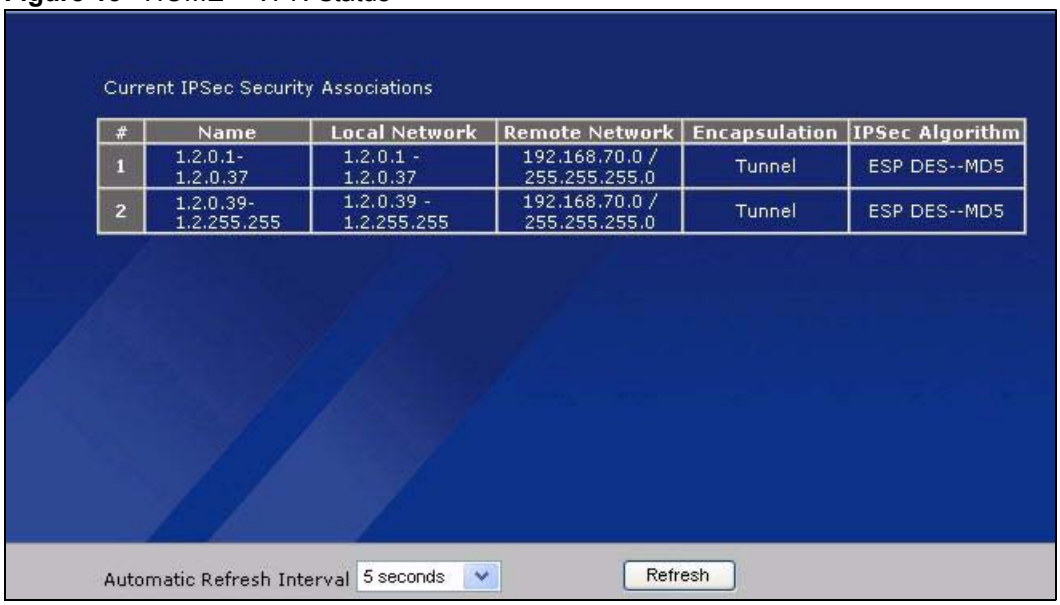
Table 9 HOME > DHCP Table

LABEL	DESCRIPTION
Interface	Select **LAN** to show the current DHCP client information for the **LAN** interface.
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyWALL always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table. After you click **Apply**, the MAC address and IP address also display in the **LAN Static DHCP** screen (where you can edit them).
Refresh	Click **Refresh** to reload the DHCP table.

2.3.9 VPN Status

Click **VPN** in the **HOME** screen when the ZyWALL is set to router mode. This screen displays read-only information about the active VPN connections. The **Poll Interval(s)** field is configurable. A Security Association (SA) is the group of security settings related to a specific VPN tunnel.

Figure 13 HOME > VPN Status


Current IPSec Security Associations
Name Local Network Remote Network Encapsulation IPSec Algorithm
1 1.2.0.1-1.2.0.37 1.2.0.1 - 1.2.0.37 192.168.70.0 / 255.255.255.0 Tunnel ESP DES--MD5
2 1.2.0.39-1.2.255.255 1.2.0.39 - 1.2.255.255 192.168.70.0 / 255.255.255.0 Tunnel ESP DES--MD5
Automatic Refresh Interval
5 seconds
Refresh

The following table describes the labels in this screen.

Table 10 HOME > VPN Status

LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Local Network	This field displays the IP address of the computer using the VPN IPSec feature of your ZyWALL.
Remote Network	This field displays IP address (in a range) of computers on the remote network behind the remote IPSec router.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase ZyWALL processing requirements and communications latency (delay).
Automatic Refresh Interval	Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh	Click this button to update the screen's statistics immediately.

3

Wizard Setup

This chapter provides information on the **Wizard Setup** screens in the web configurator. The Internet access wizard is only applicable when the ZyWALL is in router mode.

3.1 Wizard Setup Overview

The web configurator's setup wizards help you configure Internet and VPN connection settings.

In the **HOME** screen, click the **Wizard** icon

to open the **Wizard Setup Welcome** screen. The following summarizes the wizards you can select:

- **Internet Access Setup:** click this link to open a wizard to set up an Internet connection for the **WAN** port. This wizard is available when the ZyWALL is in router or zero configuration mode, not when it is in bridge mode.
- **VPN Setup:** click this link to configure a VPN connection that uses a pre-shared key. If you want to set the rule to use a certificate, please go to the VPN screens for configuration. See Section 3.3 on page 71.

Figure 14 Wizard Setup Welcome

Welcome to the ZyWALL Wizard Setup
Internet Access Setup
(helps user quickly configure the ZyWALL P1 to secure Internet connection)
VPN Setup
(helps user quickly configure the ZyWALL P1 to secure VPN connection)
Close

3.2 Internet Access

The Internet access wizard screen has three variations depending on what encapsulation type you use. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don’t have that information.

3.2.1 ISP Parameters

The ZyWALL offers three choices of encapsulation. They are **Ethernet**, **PPTP** or **PPPoE**.

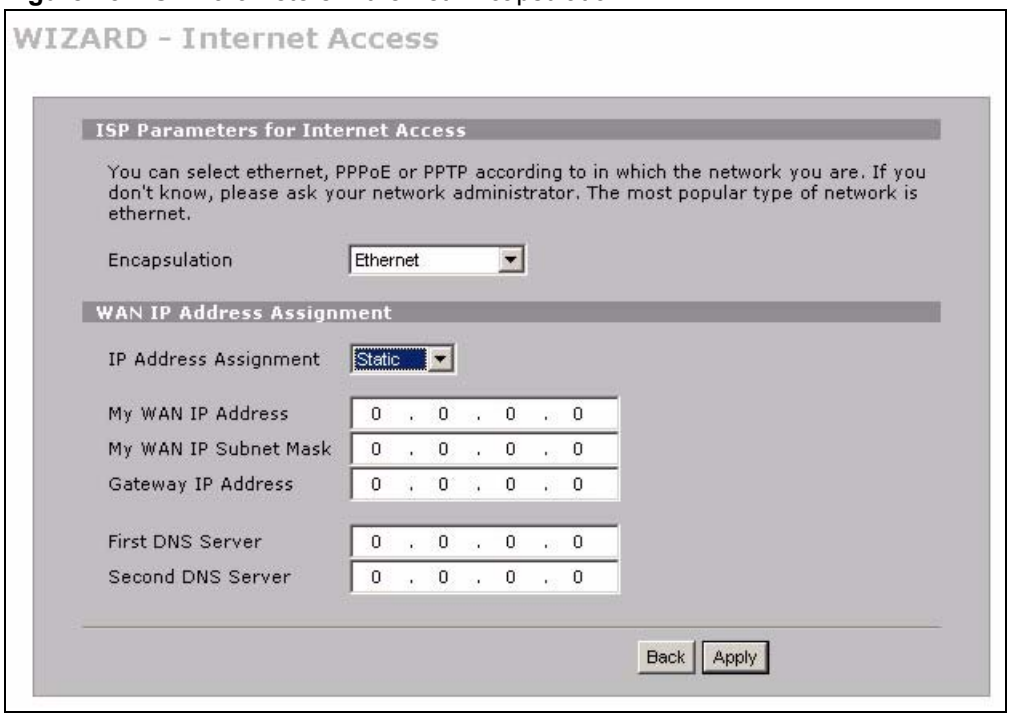
The wizard screen varies according to the type of encapsulation that you select in the **Encapsulation** field.

3.2.1.1 Ethernet

For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a **WAN-to-WAN/ZyWALL** firewall rule for those packets. Contact your ISP to find the correct port number.

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

Figure 15 ISP Parameters: Ethernet Encapsulation


WIZARD - Internet Access
ISP Parameters for Internet Access
You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.
Encapsulation
Ethernet
WAN IP Address Assignment
IP Address Assignment
Static
My WAN IP Address
My WAN IP Subnet Mask
Gateway IP Address
First DNS Server
Second DNS Server
0 . 0 . 0 . 0
Back
Apply

The following table describes the labels in this screen.

Table 11 ISP Parameters: Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection.
WAN IP Address Assignment	
IP Address Assignment	Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection. Select **Static** If the ISP assigned a fixed IP address. The fields below are available only when you select **Static**.

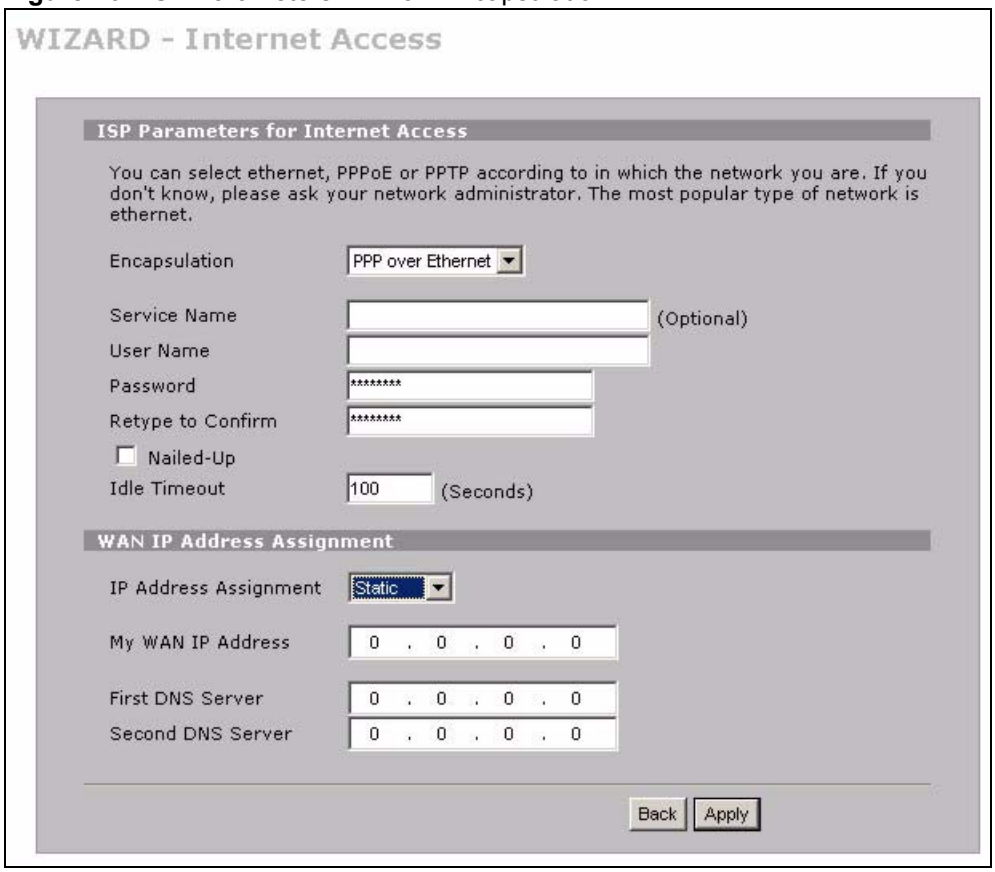
Table 11 ISP Parameters: Ethernet Encapsulation

LABEL	DESCRIPTION
My WAN IP Address	Enter your WAN IP address in this field.
My WAN IP Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address	Enter the gateway IP address in this field.
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Back	Click **Back** to return to the previous wizard screen.
Apply	Click **Apply** to save your changes and go to the next screen.

3.2.1.2 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

Figure 16 ISP Parameters: PPPoE Encapsulation


WIZARD - Internet Access
ISP Parameters for Internet Access
You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.
Encapsulation
PPP over Ethernet
Service Name
(Optional)
User Name
Password
Retype to Confirm
Nailed-Up
Idle Timeout
100
(Seconds)
WAN IP Address Assignment
IP Address Assignment
Static
My WAN IP Address
0 . 0 . 0 . 0
First DNS Server
0 . 0 . 0 . 0
Second DNS Server
0 . 0 . 0 . 0
Back
Apply

The following table describes the labels in this screen.

Table 12 ISP Parameters: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Encapsulation	Choose an encapsulation method from the pull-down list box. **PPP over Ethernet** forms a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is **100** seconds.
WAN IP Address Assignment	
IP Address Assignment	Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection. Select **Static** If the ISP assigned a fixed IP address. The fields below are available only when you select **Static**.
My WAN IP Address	Enter your WAN IP address in this field.
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Back	Click **Back** to return to the previous wizard screen.
Apply	Click **Apply** to save your changes and go to the next screen.

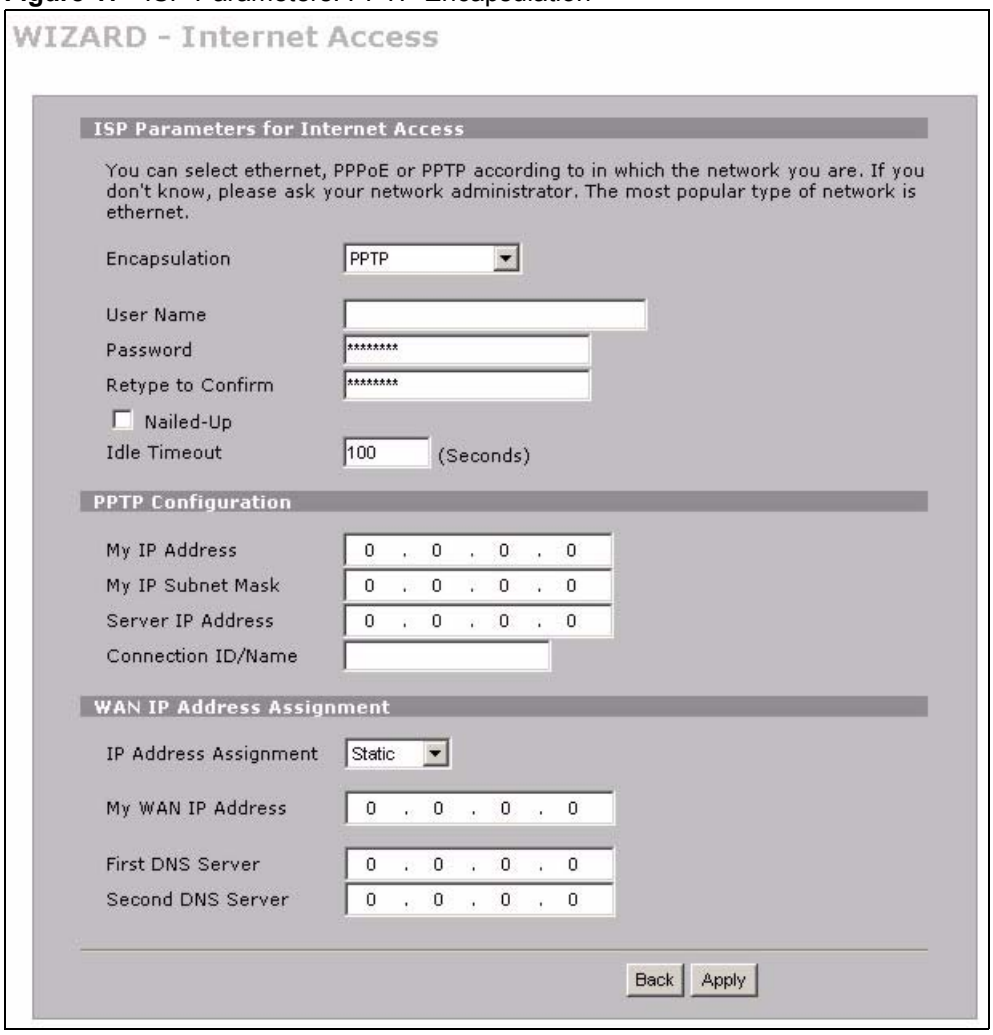
3.2.1.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

The ZyWALL supports one PPTP server connection at any given time.

Figure 17 ISP Parameters: PPTP Encapsulation



The following table describes the labels in this screen.

Table 13 ISP Parameters: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select **PPTP** from the drop-down list box. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.

Table 13 ISP Parameters: PPTP Encapsulation

LABEL	DESCRIPTION
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your xDSL modem.
WAN IP Address Assignment	
IP Address Assignment	Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection. Select **Static** If the ISP assigned a fixed IP address. The fields below are available only when you select **Static**.
My WAN IP Address	Enter your WAN IP address in this field.
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Back	Click **Back** to return to the previous wizard screen.
Apply	Click **Apply** to save your changes and go to the next screen.

3.2.2 Internet Access Wizard: Second Screen

Click **Next** to go to the screen where you can register your ZyWALL and activate the free anti-virus and IDP trial applications.

Otherwise, click **Skip** to display the congratulations screen and click **Close** to complete the Internet access setup.

Figure 18 Internet Access Wizard: Second Screen

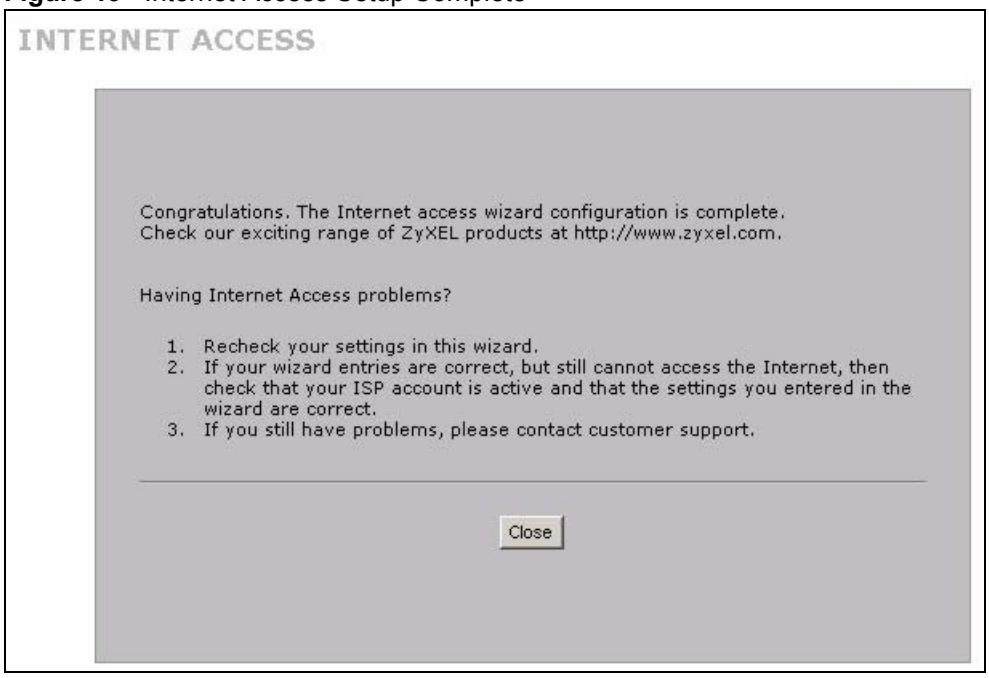
INTERNET ACCESS
Product registration and service activation for free
You can register ZyWALL on http://www.myzyxel.com and activate "Free Trial" of AntiVirus and IDP services on your ZyWALL.
Click "Next" to activate these services for FREE.
Skip
Next

3.2.3 Internet Access Wizard: Wizard Finish

Well done! You have finished configuration using the Internet Access Wizard. You may now test your Internet connection.

You can now close the wizard.

Figure 19 Internet Access Setup Complete


INTERNET ACCESS
Congratulations. The Internet access wizard configuration is complete.
Check our exciting range of ZyXEL products at http://www.zyxel.com.
Having Internet Access problems?
1. Recheck your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.
Close

3.2.4 Internet Access Wizard: Registration

If you clicked **Next** in the previous screen (see Figure 18 on page 66), the following screen displays.

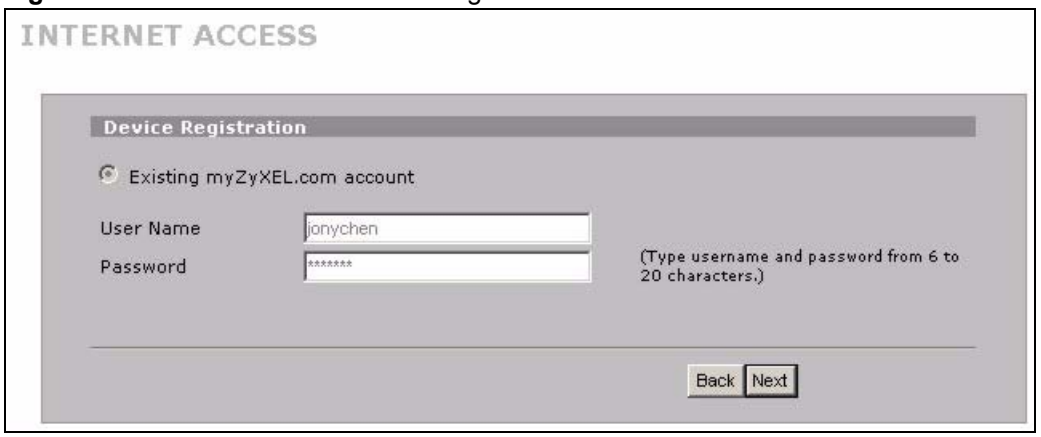
Use this screen to register the ZyWALL with myZyXEL.com. You must register your ZyWALL before you can activate trial applications of anti-virus and IDP services.

- You must be connected to the Internet to register.
- This screen displays a read-only user name and password if the ZyWALL is already registered. It also shows which trial services are activated (if any). You can still select the unchecked trial service(s) to activate it after registration. Use the **Registration > Service** screen to update your service subscription status.

Figure 20 Internet Access Wizard: Registration

If the ZyWALL has been registered, this screen is read-only and just displays your user name and password.

Figure 21 Internet Access Wizard: Registered Device



The following table describes the labels in this screen.

Table 14 Internet Access Wizard: Registration

LABEL	DESCRIPTION
Device Registration	If you select **Existing myZyXEL.com account**, only the **User Name** and **Password** fields are available.
New myZyXEL.com account	If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your ZyWALL.
Existing myZyXEL.com account	If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your ZyWALL.
User Name	Enter a user name for your myZyXEL.com account. The name should be from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Check	Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used.

Table 14 Internet Access Wizard: Registration

LABEL	DESCRIPTION
Password	Enter a password of between six and 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Confirm Password	Enter the password again for confirmation.
E-Mail Address	Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces.
Country	Select your country from the drop-down box list.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

After you fill in the fields and click **Next**, the following screen shows indicating the registration is in progress. Wait for the registration progress to finish.

Figure 22 Internet Access Wizard: Registration in Progress

This screen appears if the registration was not successful. Click **Return** to go back to the **Device Registration** screen and check your settings.

Figure 23 Internet Access Wizard: Registration Failed

3.2.5 Internet Access Wizard: Service Activation

Use this screen to activate trial periods of subscription security features if you have not already done so.

You can try a trial service subscription. After the trial expires, you can buy an iCard and enter the license key in the Registration Service screen to extend the service.

Figure 24 Service Activation

If the ZyWALL has already been registered, the **Service Activation** screen indicates what trial applications are activated.

Figure 25 Internet Access Wizard: Activated Services

The following table describes the labels in this screen.

Table 15 Service Activation

LABEL	DESCRIPTION
IDP/AV 3-month Trial	Select the check box to activate a trial. The trial period starts the day you activate the trial.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to save your changes back to the ZyWALL and activate the selected services.

After you select the service and click **Next**, the following screen shows indicating the service registration is in progress. Wait for the registration progress to finish.

Figure 26 Internet Access Wizard: Registration in Progress

3.2.6 Internet Access Wizard: Status

This screen displays when the registration and activation are done. Click **Close** to leave the wizard screens.

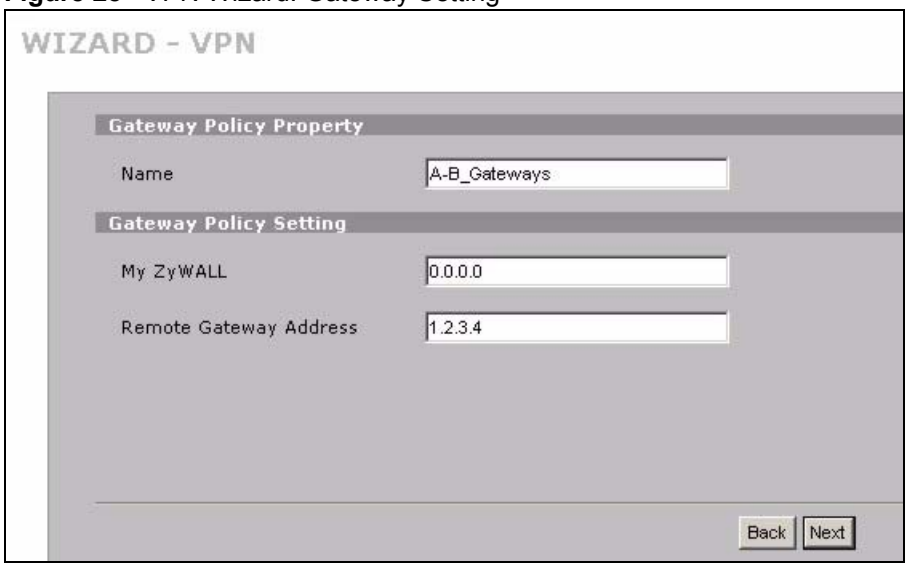
Figure 27 Internet Access Wizard: Status

3.3 VPN Wizard Gateway Setting

Use this screen to name the VPN gateway policy (IKE SA) and identify the IPSec routers at either end of the VPN tunnel.

Click **VPN Setup** in the **Wizard Setup Welcome** screen (Figure 14 on page 61) to open the VPN configuration wizard. The first screen displays as shown next.

Figure 28 VPN Wizard: Gateway Setting



The following table describes the labels in this screen.

Table 16 VPN Wizard: Gateway Setting

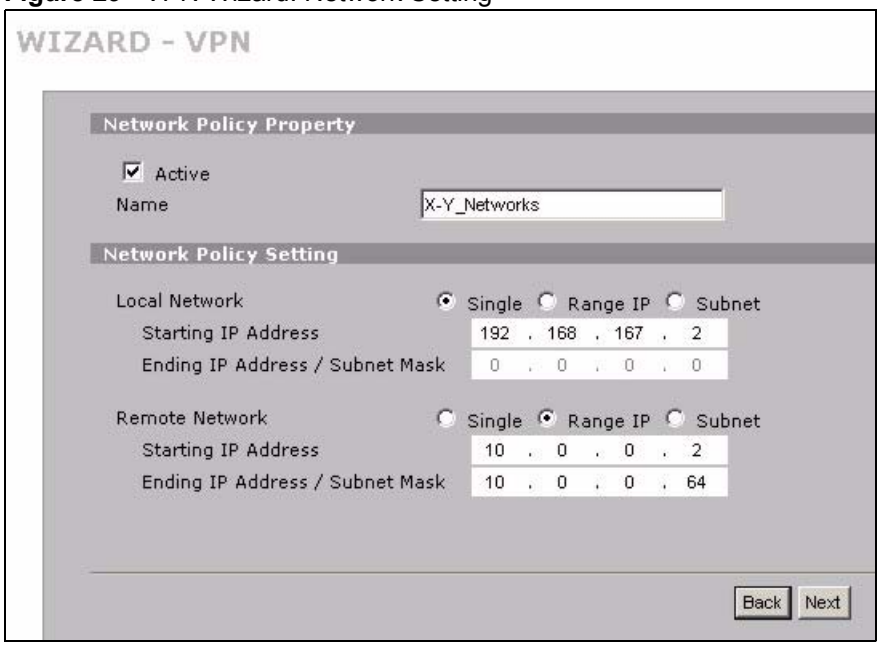
LABEL	DESCRIPTION
Gateway Policy Property	
Name	Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
My ZyWALL	When the ZyWALL is in router mode, enter the WAN IP address or the domain name of your ZyWALL or leave the field set to **0.0.0.0**. The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. The VPN tunnel has to be rebuilt if this IP address changes. When the ZyWALL is in bridge mode, this field is read-only and displays the ZyWALL's IP address.
Remote Gateway Address	Enter the WAN IP address or domain name of the remote IPSec router (secure gateway) in the field below to identify the remote IPSec router by its IP address or a domain name. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.4 VPN Wizard Network Setting

Use this screen to name the VPN network policy (IPSec SA) and identify the devices behind the IPSec routers at either end of a VPN tunnel.

Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.

Figure 29 VPN Wizard: Network Setting



The following table describes the labels in this screen.

Table 17 VPN Wizard: Network Setting

LABEL	DESCRIPTION
Network Policy Property	
Active	If the **Active** check box is selected, packets for the tunnel trigger the ZyWALL to build the tunnel. Clear the **Active** check box to turn the network policy off. The ZyWALL does not apply the policy. Packets for the tunnel do not trigger the tunnel.
Name	Type up to 32 characters to identify this VPN network policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Network Policy Setting	
Local Network	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Select **Single** for a single IP address. Select **Range IP** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Local Network** field is configured to **Single**, enter a (static) IP address on the LAN behind your ZyWALL. When the **Local Network** field is configured to **Range IP**, enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Local Network** field is configured to **Subnet**, this is a (static) IP address on the LAN behind your ZyWALL.
Ending IP Address/ Subnet Mask	When the **Local Network** field is configured to **Single**, this field is N/A. When the **Local Network** field is configured to **Range IP**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Local Network** field is configured to **Subnet**, this is a subnet mask on the LAN behind your ZyWALL.
Remote Network	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. Select **Single** for a single IP address. Select **Range IP** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.

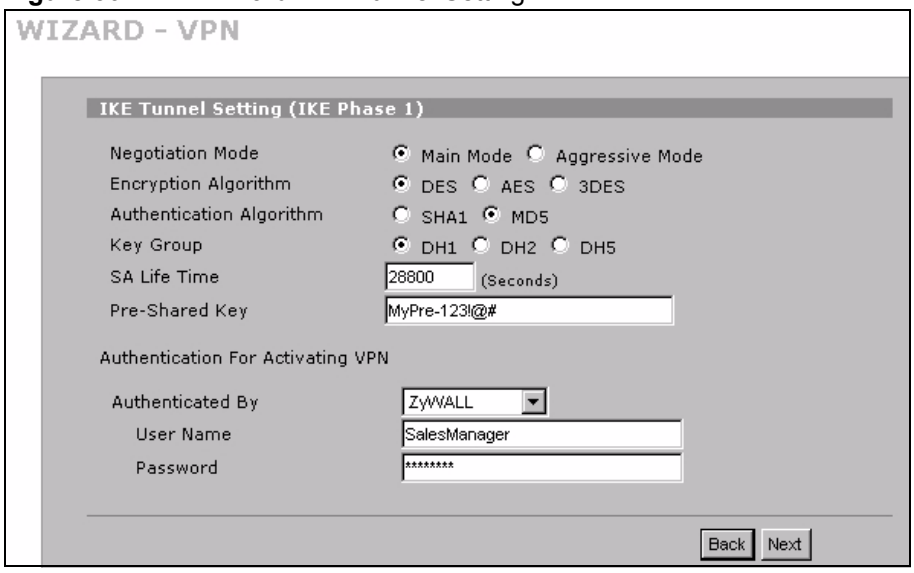
Table 17 VPN Wizard: Network Setting

LABEL	DESCRIPTION
Starting IP Address	When the **Remote Network** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Network** field is configured to **Range IP**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Network** field is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router
Ending IP Address/ Subnet Mask	When the **Remote Network** field is configured to **Single**, this field is N/A. When the **Remote Network** field is configured to **Range IP**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Network** field is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.5 VPN Wizard IKE Tunnel Setting (IKE Phase 1)

Use this screen to specify the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA.

Figure 30 VPN Wizard: IKE Tunnel Setting



The following table describes the labels in this screen.

Table 18 VPN Wizard: IKE Tunnel Setting

LABEL	DESCRIPTION
Negotiation Mode	Select **Main Mode** for identity protection. Select **Aggressive Mode** to allow more incoming connections from dynamic IP addresses to use separate passwords. Note: Multiple SAs (security associations) connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**.
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. **DH5** refers to Diffie-Hellman Group 5 a 1536-bit random number.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
Authenticated By	Select **XAUTH** to have the remote IPSec router authenticate user(s) that request this VPN connection. Note: You must also configure extended authentication on the remote IPsec router. Select **ZyWALL** to have your ZyWALL authenticate user(s) using a username and password when initiating this VPN connection. Select this option if the remote IPSec router is not configured to authenticate VPN user or does not have the extended authentication function. Select **None** to not authenticate user(s) that request this VPN connection.

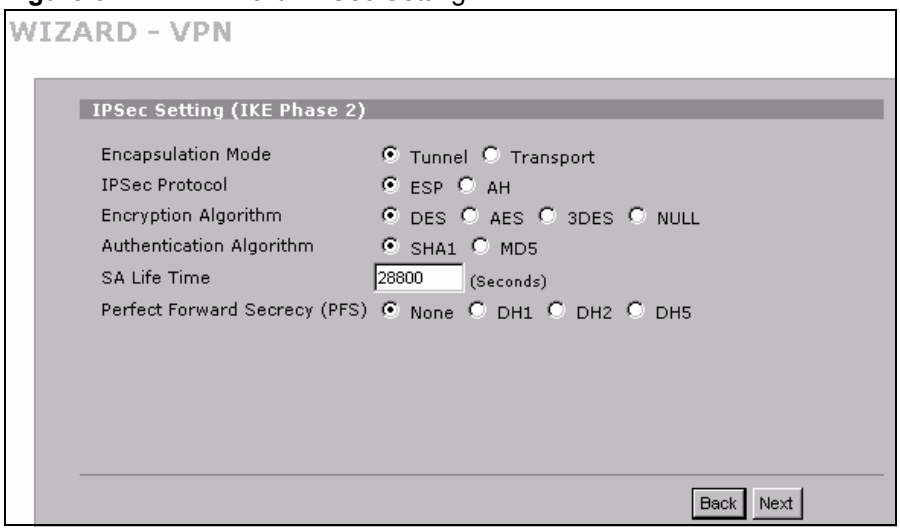
Table 18 VPN Wizard: IKE Tunnel Setting (continued)

LABEL	DESCRIPTION
User Name	Enter a user name for your ZyWALL to be authenticated by the VPN peer (in server mode). The user name can be up to 31 case-sensitive ASCII characters, but spaces are not allowed. You must enter a user name and password when you select client mode.
Password	Enter the corresponding password for the above user name. The password can be up to 31 case-sensitive ASCII characters, but spaces are not allowed.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.6 VPN Wizard IPSec Setting (IKE Phase 2)

Use this screen to specify the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.

Figure 31 VPN Wizard: IPSec Setting



The following table describes the labels in this screen.

Table 19 VPN Wizard: IPSec Setting

LABEL	DESCRIPTION
Encapsulation Mode	**Tunnel** is compatible with NAT, **Transport** is not. Tunnel mode encapsulates the entire IP packet to transmit it securely. A Tunnel mode is required for gateway services to provide access to internal systems. Tunnel mode is fundamentally an IP tunnel with authentication and encryption. Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In Transport mode, the IP packet contains the security protocol (AH or ESP) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).
IPSec Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay).

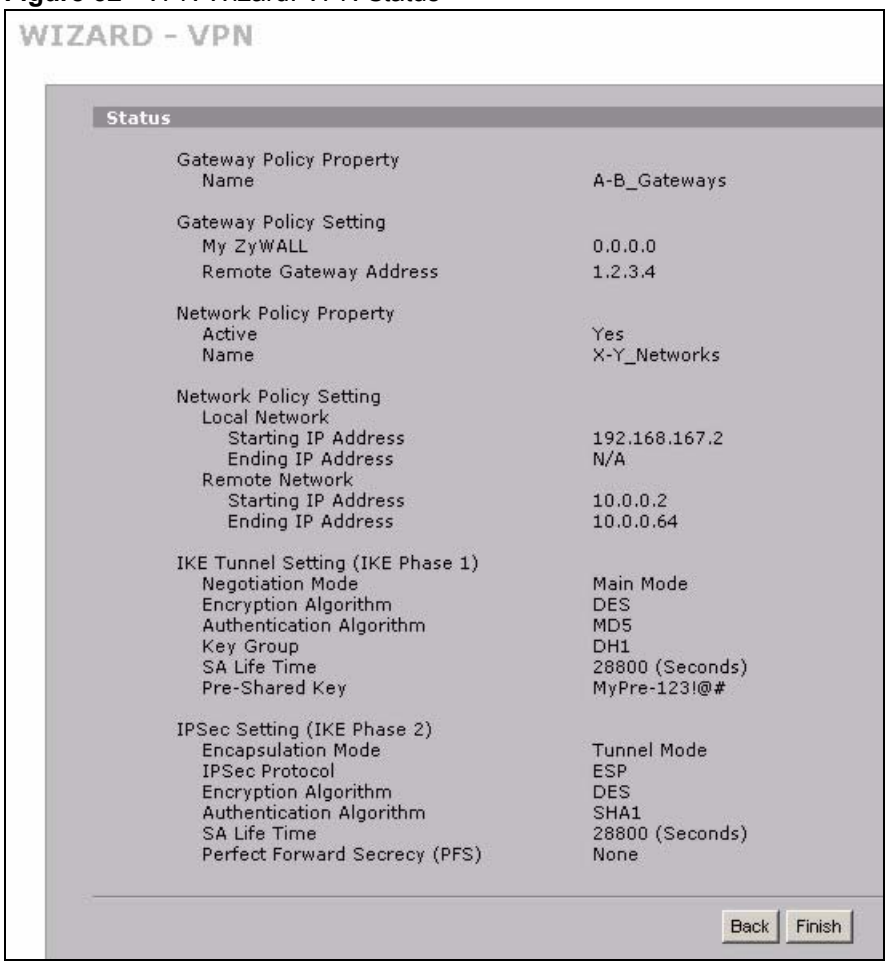
Table 19 VPN Wizard: IPSec Setting (continued)

LABEL	DESCRIPTION
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Select **DH1**, **DH2** or **DH5** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower). **DH5** refers to Diffie-Hellman Group 5 a 1536-bit random number.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.7 VPN Wizard Status Summary

This read-only screen shows the VPN settings. Use the summary table to check whether what you have configured is correct.

Figure 32 VPN Wizard: VPN Status



The following table describes the labels in this screen.

Table 20 VPN Wizard: VPN Status

LABEL	DESCRIPTION
Gateway Policy Property	
Name	This is the name of this VPN gateway policy.
Gateway Policy Setting	
My ZyWALL	This is the WAN IP address or the domain name of your ZyWALL in router mode or the ZyWALL's IP address in bridge mode.
Remote Gateway Address	This is the IP address or the domain name used to identify the remote IPSec router.
Network Policy Property	
Active	This displays whether this VPN network policy is enabled or not.
Name	This is the name of this VPN network policy.
Network Policy Setting	
Local Network	

Table 20 VPN Wizard: VPN Status (continued)

LABEL	DESCRIPTION
Starting IP Address	This is a (static) IP address on the LAN behind your ZyWALL.
Ending IP Address/ Subnet Mask	When the local network is configured for a single IP address, this field is N/A. When the local network is configured for a range IP address, this is the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the local network is configured for a subnet, this is a subnet mask on the LAN behind your ZyWALL.
Remote Network	
Starting IP Address	This is a (static) IP address on the network behind the remote IPSec router.
Ending IP Address/ Subnet Mask	When the remote network is configured for a single IP address, this field is N/A. When the remote network is configured for a range IP address, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the remote network is configured for a subnet, this is a subnet mask on the network behind the remote IPSec router.
IKE Tunnel Setting (IKE Phase 1)	
Negotiation Mode	This shows **Main Mode** or **Aggressive Mode**. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	This is the method of data encryption. Options can be **DES**, **3DES** or **AES**.
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data.
Key Group	This is the key group you chose for phase 1 IKE setup.
SA Life Time (Seconds)	This is the length of time before an IKE SA automatically renegotiates.
Pre-Shared Key	This is a pre-shared key identifying a communicating party during a phase 1 IKE negotiation.
IPSec Setting (IKE Phase 2)	
Encapsulation Mode	This shows **Tunnel** mode or **Transport** mode.
IPSec Protocol	**ESP** or **AH** are the security protocols used for an SA.
Encryption Algorithm	This is the method of data encryption. Options can be **DES**, **3DES**, **AES** or **NULL**.
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data.
SA Life Time (Seconds)	This is the length of time before an IKE SA automatically renegotiates.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. Otherwise, **DH1**, **DH2** or **DH5** are selected to enable PFS.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to complete and save the wizard setup.

3.8 VPN Wizard Setup Complete

Congratulations! You have successfully set up the VPN rule for your ZyWALL. If you already had VPN rules configured, the wizard adds the new VPN rule after the last existing VPN rule.

Figure 33 VPN Wizard Setup Complete

WIZARD - VPN
Congratulations. The VPN wizard configuration is complete.
Check our exciting range of ZyXEL products at http://www.zyxel.com
Having VPN access problems?
1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.
Close

4

Tutorial

This chapter gives examples of how to configure some of your ZyWALL's key features. See the related chapter on a feature for more details.

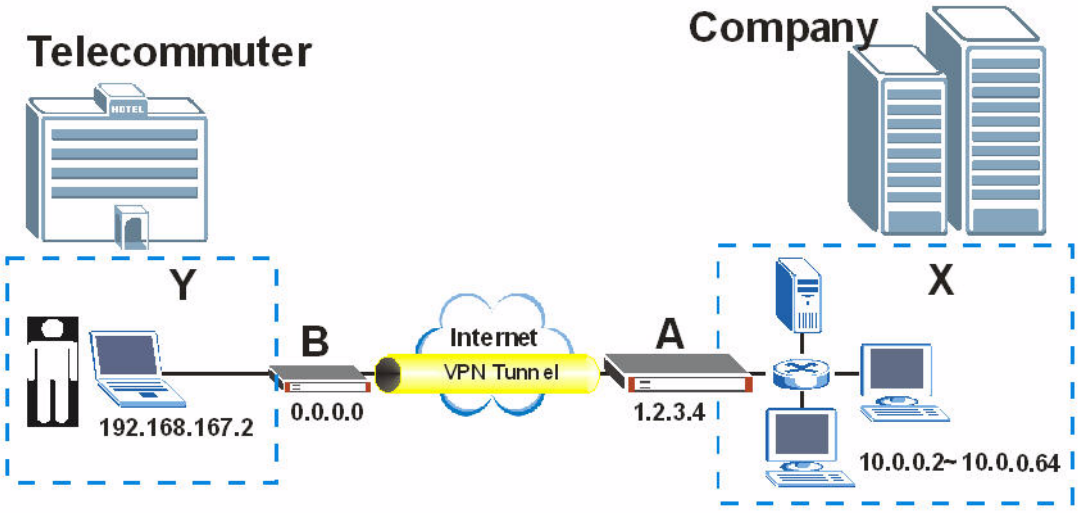
4.1 Dynamic VPN Rule Configuration

Dynamic VPN rules allow VPN connections from IPSec routers with dynamic WAN IP addresses. This tutorial shows how to configure a basic VPN (Virtual Private Network) tunnel to allow a traveling sales manager named Bob (**Y** in the figure) using a ZyWALL P1 (**B**) to securely connect to computers and servers on the office network **X** behind a ZyWALL 70 (**A**).

- The ZyWALLs are peers.
- ZyWALL **B** has a dynamically-assigned WAN IP addresses (represented by 0.0.0.0), so only ZyWALL **B** can initiate (trigger) the VPN tunnel.

ZyWALL **B** automatically initiates a VPN tunnel to ZyWALL A whenever **Y** tries to connect to an IP address from 10.0.0.2 to 10.0.0.64 and passes the identification authentication.

Figure 34 Dynamic VPN Rule Example



This example uses the following settings.

Table 21 Dynamic VPN Rule Tutorial Settings

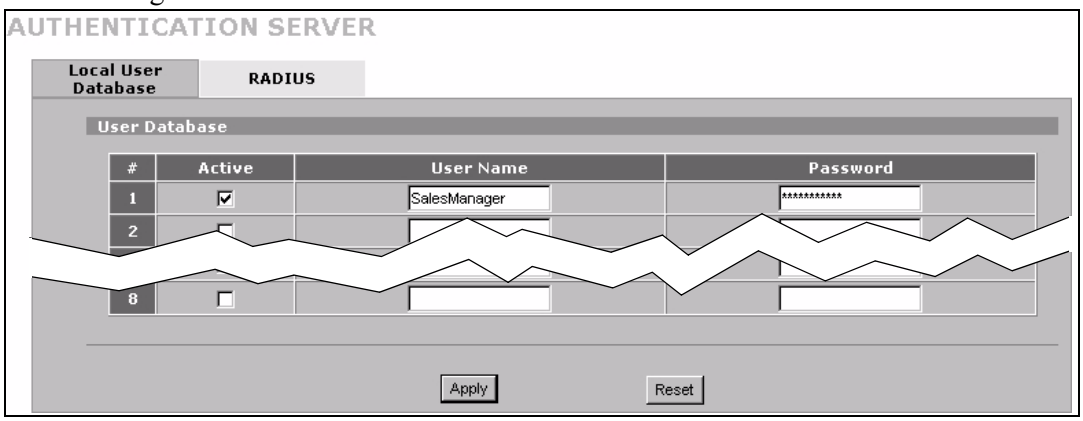
FIELD	ZYWALL A (COMPANY)	ZYWALL B (BOB)
Gateway Policy Property Name (identifies the VPN rule)	A-B_Gateways	A-B_Gateways
MyZyWALL (ZyWALL's WAN IP address)	1.2.3.4	0.0.0.0
Remote Gateway Address (peer ZyWALL's WAN IP address)	0.0.0.0	1.2.3.4
Network Policy Property Name (name of the policy that identifies the networks behind the ZyWALLs)	X-Y_Networks	X-Y_Networks
Local Network (network behind the local ZyWALL) Note: Use static IP addresses or static DHCP to make sure the computers behind the ZyWALLs always use these IP addresses.	10.0.0.2 ~10.0.0.64	192.168.167.2
Remote Network (network behind the peer ZyWALL)	0.0.0.0	10.0.0.2 ~10.0.0.64
Pre-Shared Key (password)	MyPre-123!@#	MyPre-123!@#
Extended Authentiation	Enable (Server Mode)	Enable (Client Mode)
Username/Password for Extended Authentiation	SalesManager/ Manager1234 (in Local User Database)	SalesManager/ Manager1234 (in VPN Gateway Policy Edit)

4.1.1 Configure Bob's User Account

This example includes extended authentication. Bob has to enter the correct username and password to use the ZyWALL tunnel. This keeps others from using Bob's ZyWALL if it is lost or stolen. ZyWALL A needs to check the VPN tunnel requests that come in from ZyWALL B. In this example, you configure a local user database account named "SalesManager" on ZyWALL A.

1 Go to **SECURITY** > **AUTH SERVER**.

2 Add and activate account for the users. In this example, enter "SalesManager" and "Manager1234".



3 Click **Apply**.

4.1.2 VPN Gateway and Network Policy Configuration

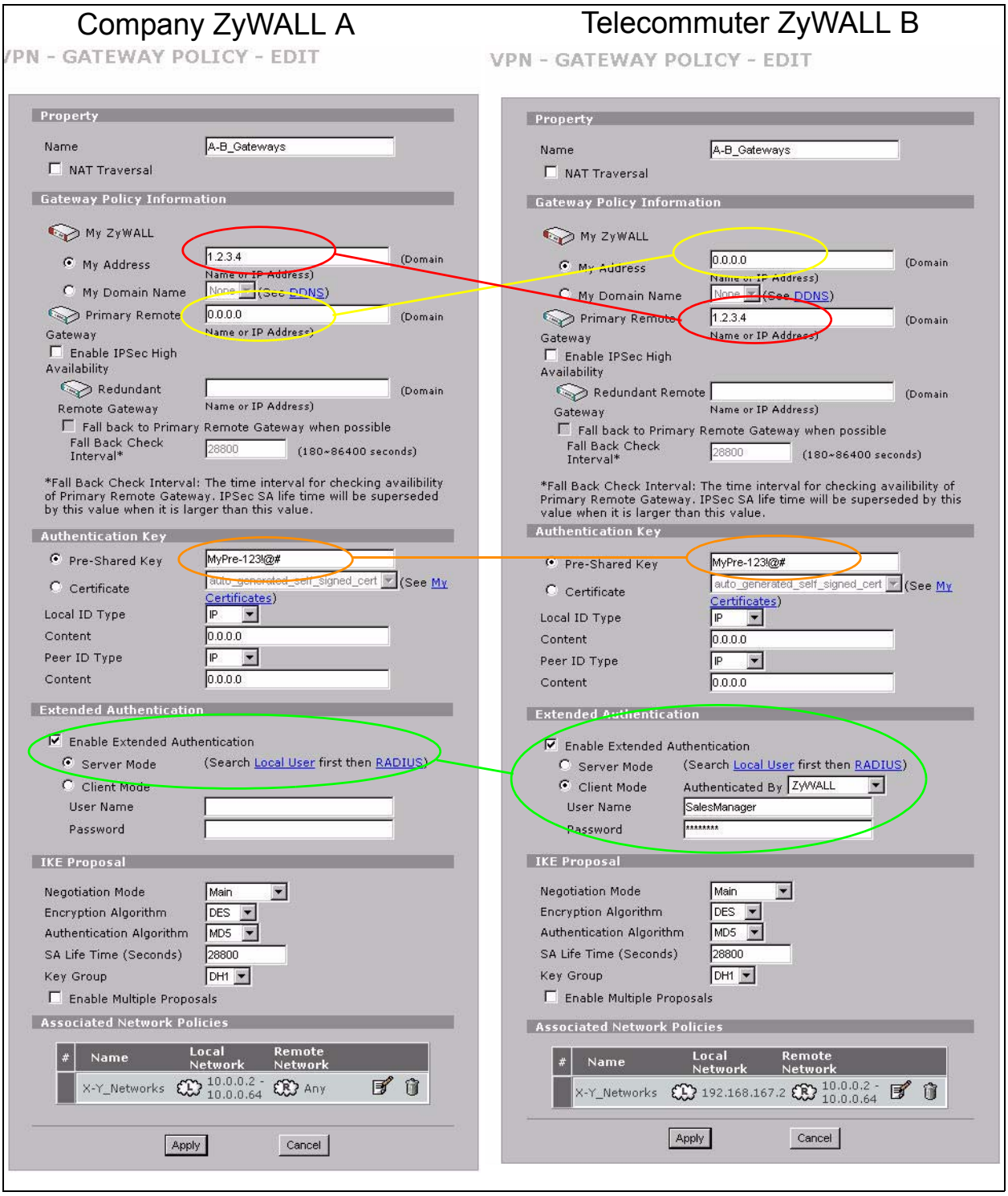
This section covers how to configure the company's ZyWALL (A) and the telecommuter's ZyWALL (B).

1 Click **SECURITY > VPN > VPN Rules (IKE)**, and then the add gateway policy ( ) icon to display the **Edit Gateway Policy** screen. Use this screen to configure the VPN gateway policy that identifies the ZyWALLs.

The company's ZyWALL (A) and the telecommuter's ZyWALL (B) gateway policy edit screens are shown next.

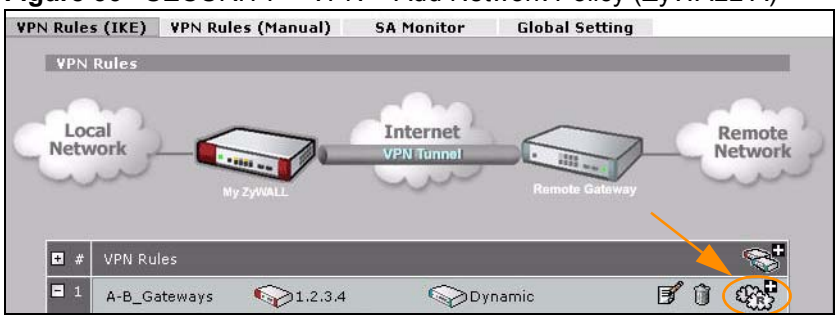
- The information that identifies the ZyWALL 70 (A) is circled in red.
- The information that identifies the ZyWALL P1 (B) is circled in yellow.
- Information that is the same in both is circled in orange.
- Extended authentication settings are in green.

Figure 35 VPN Gateway Policy Edit Screens



2 After you click **Apply**, the A-B_Gateways gateway policy displays as shown next. Click **SECURITY > VPN** and the A-B_Gateways' add network policy ( ) icon. The following figure shows ZyWALL A's screen.

Figure 36 SECURITY > VPN > Add Network Policy (ZyWALL A)

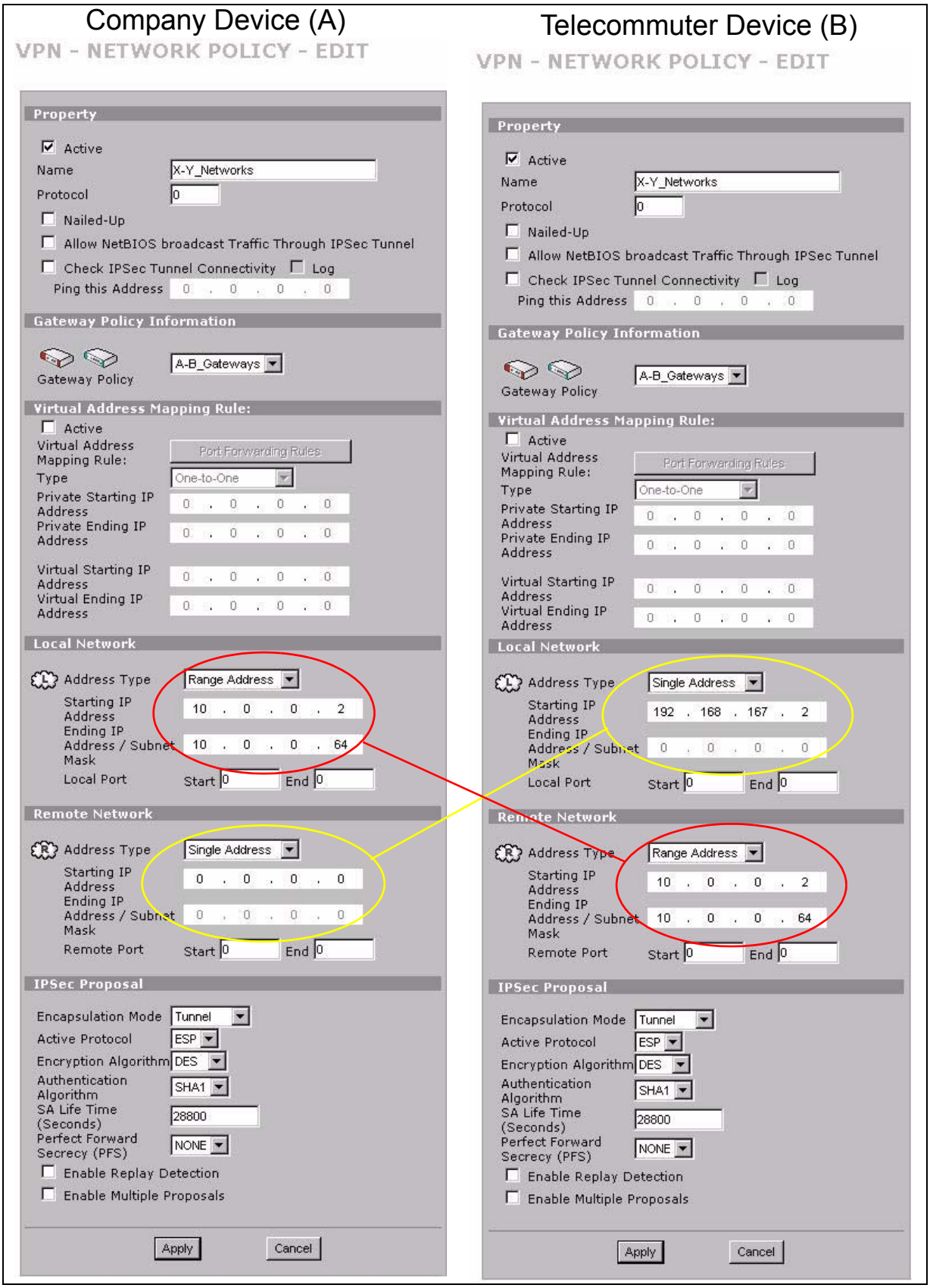


3 Edit the **VPN-Network Policy -Edit** screen to configure network policies. A network policy identifies the devices behind the IPSec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.

Here are the company's ZyWALL (A) and the telecommuter's ZyWALL (B) network policy edit screens.

- The information that identifies network X is circled in red.
- The information that identifies network Y is circled in yellow.

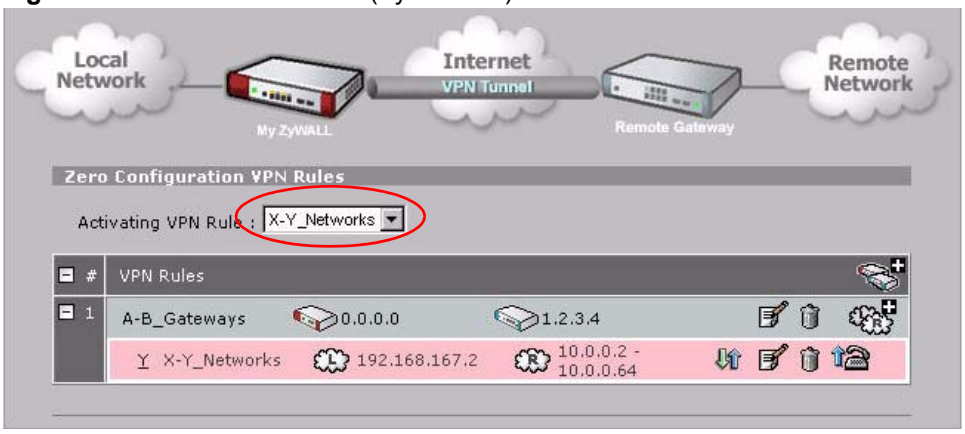
Figure 37 VPN Network Policy Edit Screens



4 After you click **Apply**, the network policy displays with the gateway policy.

5 In the ZyWALL B, select "X-Y_Networks" from the **Activating VPN Rule** field to activate the VPN rule. The color of "X-Y_Networks" VPN policy changes to pink.

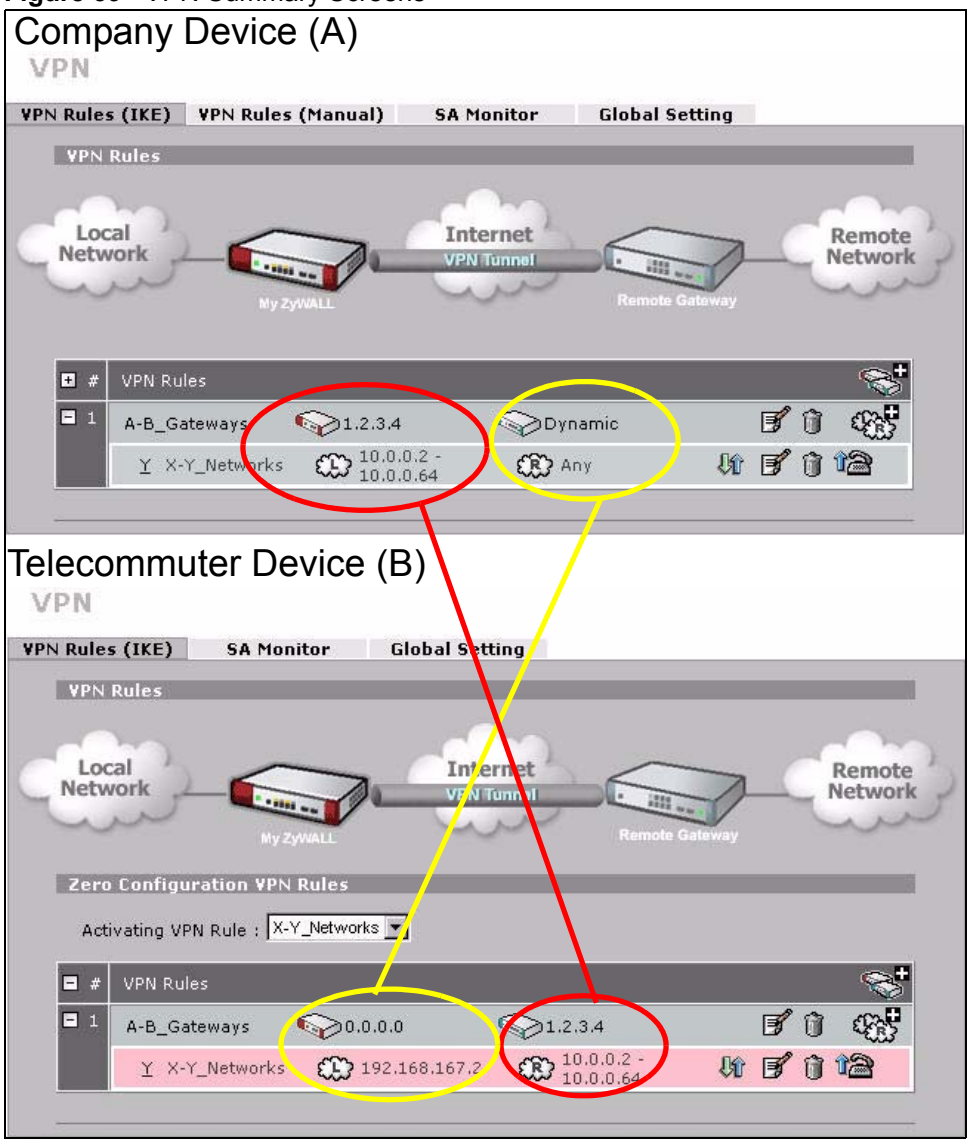
Figure 38 Activate VPN Rule (ZyWALL B)



6 Review the settings on both ZyWALLs as shown next.

- The information that identifies the ZyWALL 70 (A) and network X is circled in red.
- The information that identifies the ZyWALL P1 (B) and network Y is circled in yellow.

Figure 39 VPN Summary Screens



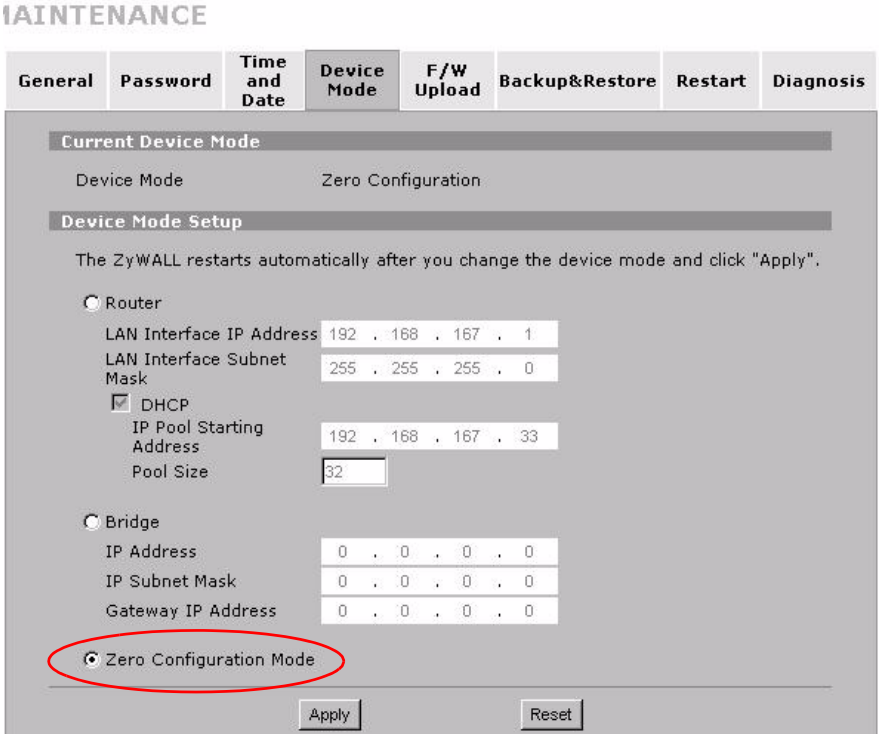
You have configured the company's ZyWALL (A) and the telecommuter's ZyWALL (B).

4.1.3 Configure Zero Configuration Mode on ZyWALL B

The ZyWALL P1's zero configuration mode provides a simplified user mode for the web configurator interface. The user uses this interface to configure the ZyWALL's Internet access settings and log into the VPN tunnel (see Section 4.1.4 on page 89). Do the following to have the telecommuter's ZyWALL (B) use zero configuration mode.

1. Log into the ZyWALL B's web configurator.
2. Go to **MAINTENANCE** and click the **Device Mode** tab.

3 Select **Zero Configuration Mode**.



4 Click **Apply**. The system reboots automatically and restarts in zero configuration mode.

4.1.4 Testing Your VPN Configuration

Test the VPN configuration before giving the ZyWALL P1 to Bob.

1 ZyWALL A should already be connected to the Internet using it's public WAN IP address. Connect ZyWALL B to the Internet. Make sure it gets a public WAN IP. You may have to take ZyWALL B to another location if it cannot get a public IP address at the company.

2 Configure one computer to use IP address192.168.167.2/24 behind the ZyWALL B. Use "ipconfig" in the command mode to ensure the IP address is properly configured.

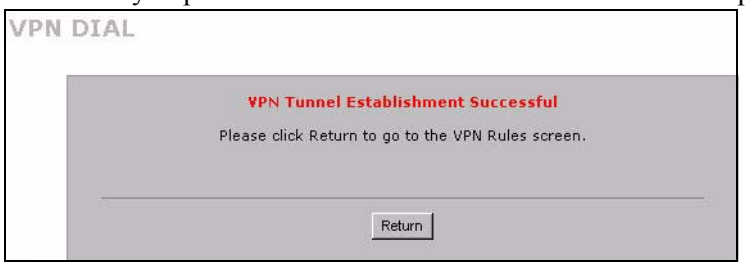
Figure 40 Check The Telecommuter's Computer IP Address

```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.167.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.167.1
```

3 Open a web browser (like Internet Explorer) to connect to the ZyWALL P1's LAN IP address (http://192.168.167.1 in this example).

4 The user mode screen for VPN authentication displays. Enter the user name "SalesManager" and password "Manager1234". Click **Activate**.

5 The ZyWALL B automatically initiates and negotiates the VPN tunnel with ZyWALL A after you pass the authentication. A successful screen displays. Click **Return**.



6 Send a ping from the telecommuter's computer (IP address 192.168.167.2) to a device on the office network (**X**), for example 10.0.0.2. You should get a response.

To do this in most Windows computers, click **Start > Run**, enter `cmd`, and then enter `ping` followed by the IP address of a computer on network **X**. Here is an example.

Figure 41 Telecommuter Pinging a Network X IP Address Example

```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=3ms TTL=126
Reply from 10.0.0.2: bytes=32 time=2ms TTL=126
Reply from 10.0.0.2: bytes=32 time=2ms TTL=126
Reply from 10.0.0.2: bytes=32 time=2ms TTL=126

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum =  3ms, Average =  2ms
```

If there is no reply to the ping, the system log can help identify a configuration problem. Click **LOGS** to see the system log. See Section 23.3.1 on page 357 for information on the log messages. You may need to click **LOGS > Log Settings** in the advanced web configurator and make sure IKE and IPSec logging is enabled at both ends. You can clear the existing log and re-attempt to build the tunnel (this makes it easier to identify the relevant logs).

When you can ping IP address 10.0.0.2 from the computer with IP address 192.168.167.2 behind ZyWALL B, you know the VPN tunnel works.

4.2 Security Settings for VPN Traffic

The ZyWALL can apply the firewall, IDP and anti-virus to the traffic going to or from VPN tunnels. The ZyWALL applies the security settings to the traffic before encrypting VPN traffic that it sends out or after decrypting received VPN traffic.

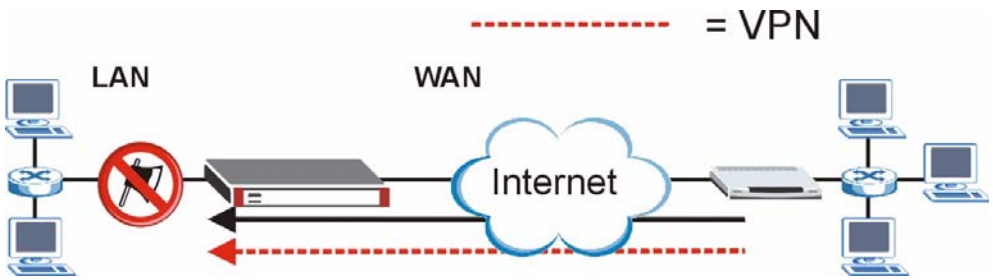
The security settings apply to VPN traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic).

You can apply firewall, IDP and anti-virus security to VPN traffic based on its direction of travel. The following examples show how you do this for IDP and the firewall.

4.2.1 IDP for From VPN Traffic Example

You can apply security settings to the **From VPN** packet direction to protect your network from attacks, intrusions, and viruses that may come in through a VPN tunnel. For example, you can use IDP to protect your LAN from intrusions that might come in through any of the VPN tunnels or interfaces.

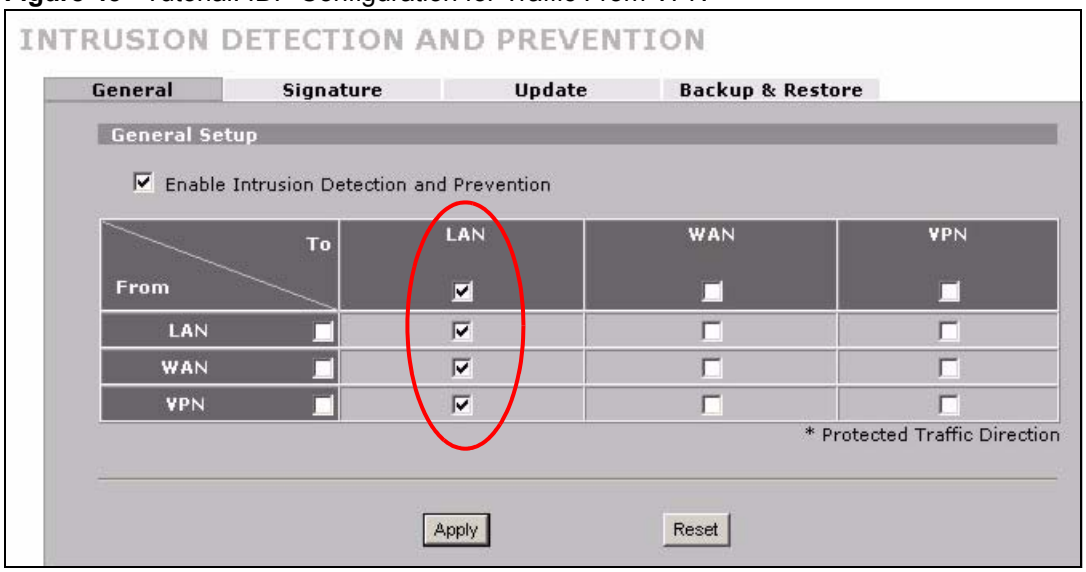
Figure 42 Tutorial: IDP for From VPN Traffic



Here is how you would configure this example.

1. Click **SECURITY > IDP > General**.
2. Select the **Enable Intrusion Detection and Prevention** check box.
3. Select the **To LAN** column's first check box (with the interface label) to select all of the **To LAN** packet directions.
4. Click **Apply**.

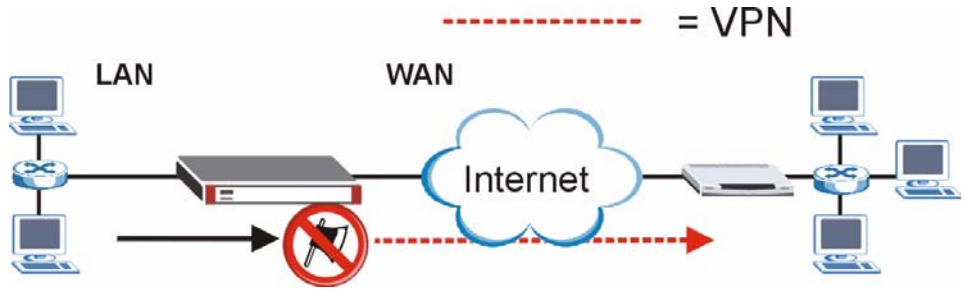
Figure 43 Tutorial: IDP Configuration for Traffic From VPN



4.2.2 IDP for To VPN Traffic Example

You can also apply security settings to the **To VPN** packet direction to protect the remote networks from attacks, intrusions, and viruses originating from your own network. For example, you can use IDP to protect the remote networks from intrusions that might come through your ZyWALL's VPN tunnel.

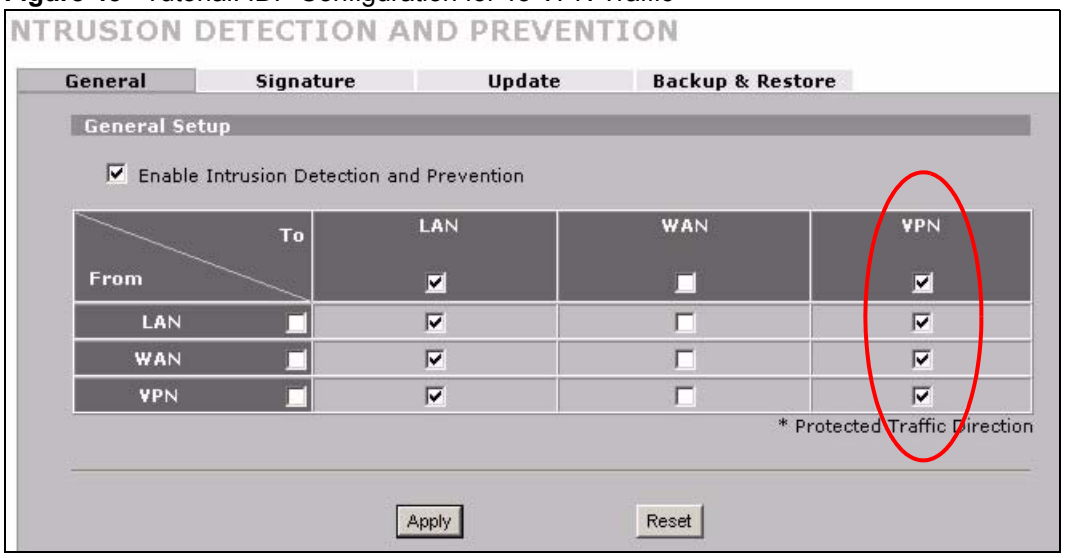
Figure 44 Tutorial: IDP for To VPN Traffic



Here is how you would configure this example.

1. Click **SECURITY > IDP > General**.
2. Select the **Enable Intrusion Detection and Prevention** check box.
3. Select the **To VPN** column's first check box (with the interface label) to select all of the **To VPN** packet directions.
4. Click **Apply**.

Figure 45 Tutorial: IDP Configuration for To VPN Traffic

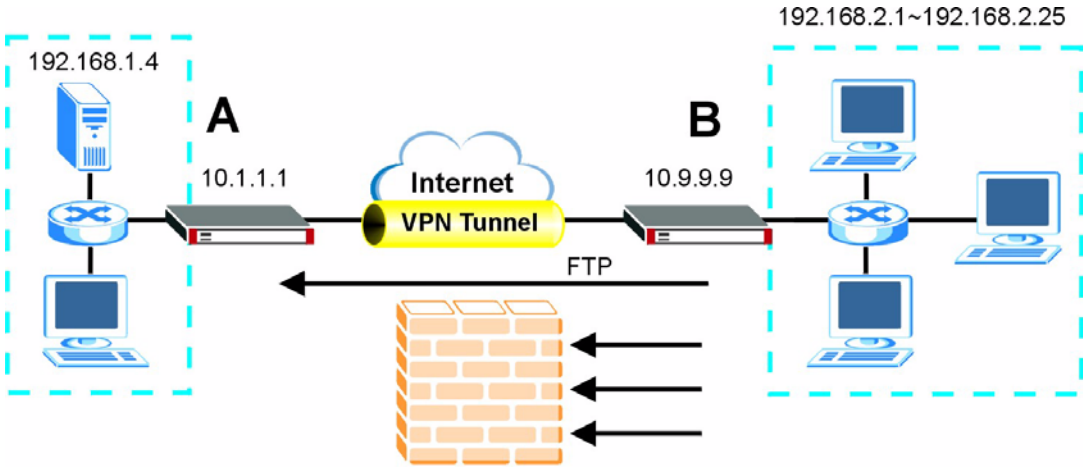


4.3 Firewall Rule for VPN Example

The firewall provides fine-tuned control for VPN tunnels. You can configure default and custom firewall rules for VPN packets.

Take the following example. You have a LAN FTP server with IP address 192.168.1.4 behind your ZyWALL (A). You could configure a VPN rule to allow the network behind device B to access your LAN FTP server through a VPN tunnel. Now, if you don't want other services like chat or e-mail going to the FTP server, you can configure firewall rules that allow only FTP traffic to come from the VPN tunnel to the FTP server.

Figure 46 Tutorial: Firewall Rule for VPN



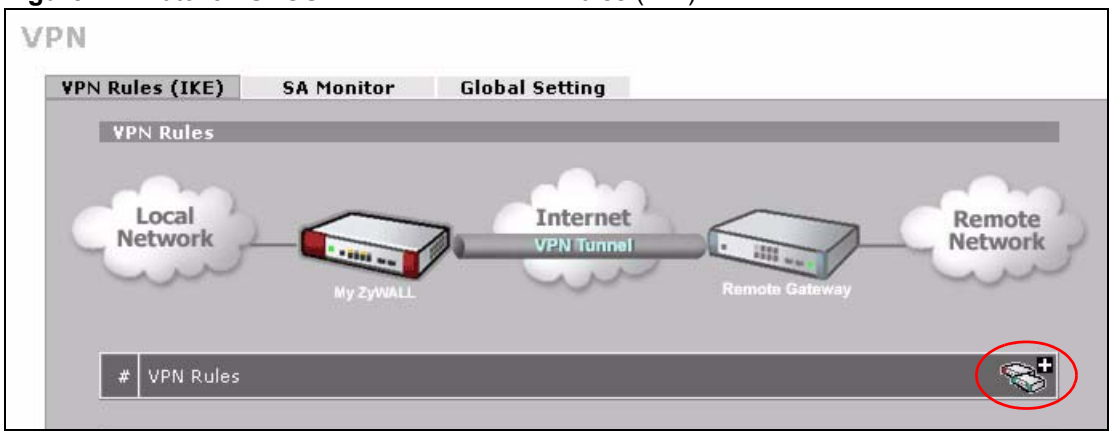
In order for devices on the remote network to initiate the VPN connection to your ZyWALL, your ZyWALL must use a static WAN IP address or DDNS (see Section 8.7 on page 136).

4.3.1 Configuring the VPN Rule

This section shows how to configure a VPN rule on device A to let the network behind B access the FTP server. You would also have to configure a corresponding rule on device B.

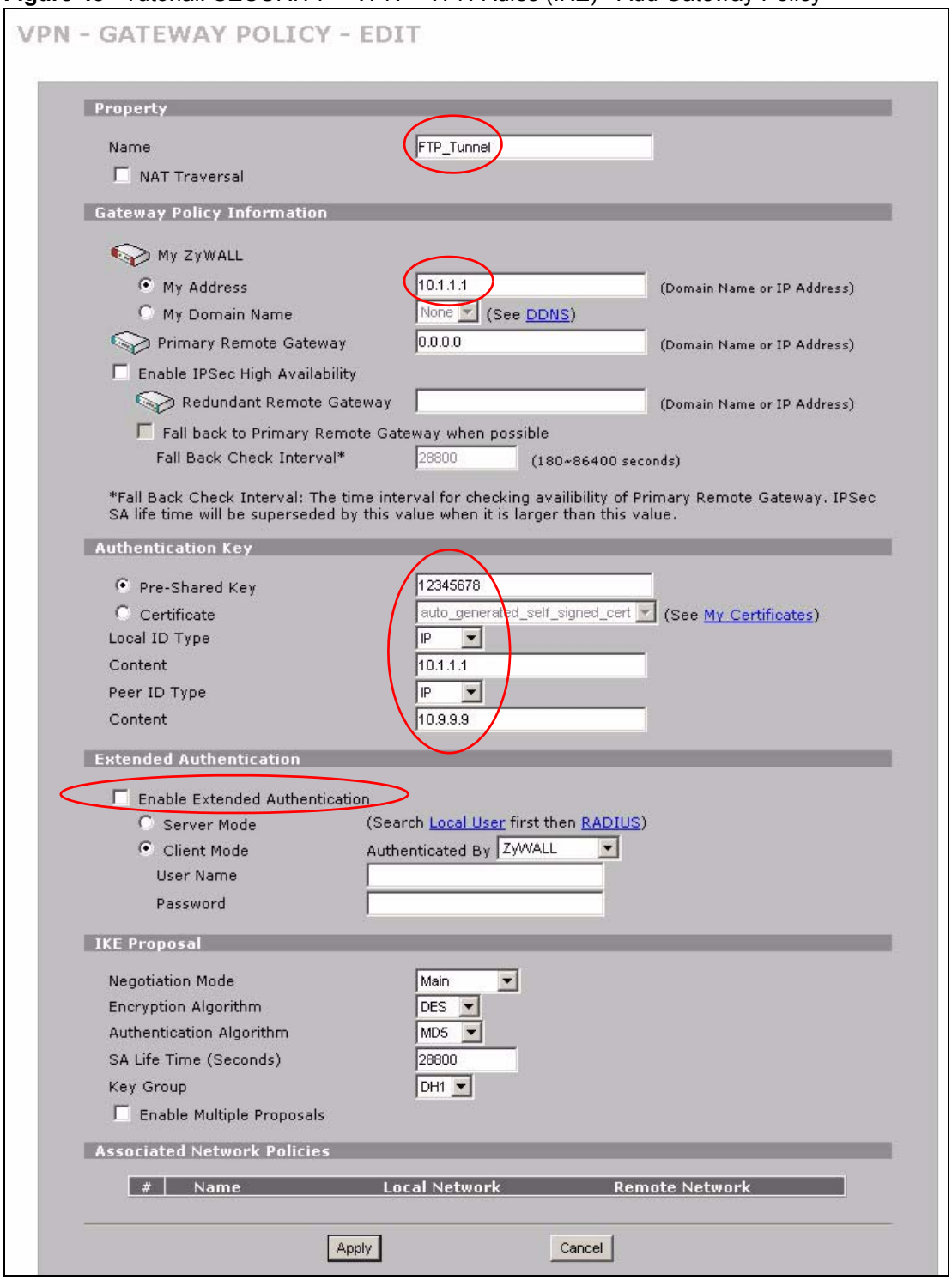
1 Click **Security > VPN** to open the following screen. Click the **Add Gateway Policy** icon.

Figure 47 Tutorial: SECURITY > VPN > VPN Rules (IKE)



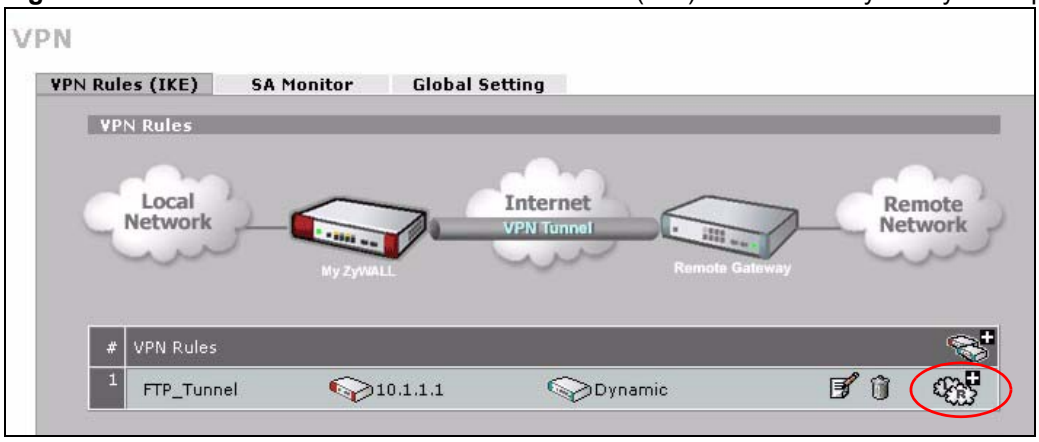
2 Use this screen to set up the connection between the routers. Configure the fields that are circled as follows and click **Apply**.

Figure 48 Tutorial: SECURITY > VPN > VPN Rules (IKE)> Add Gateway Policy



3 Click the **Add Network Policy** icon.

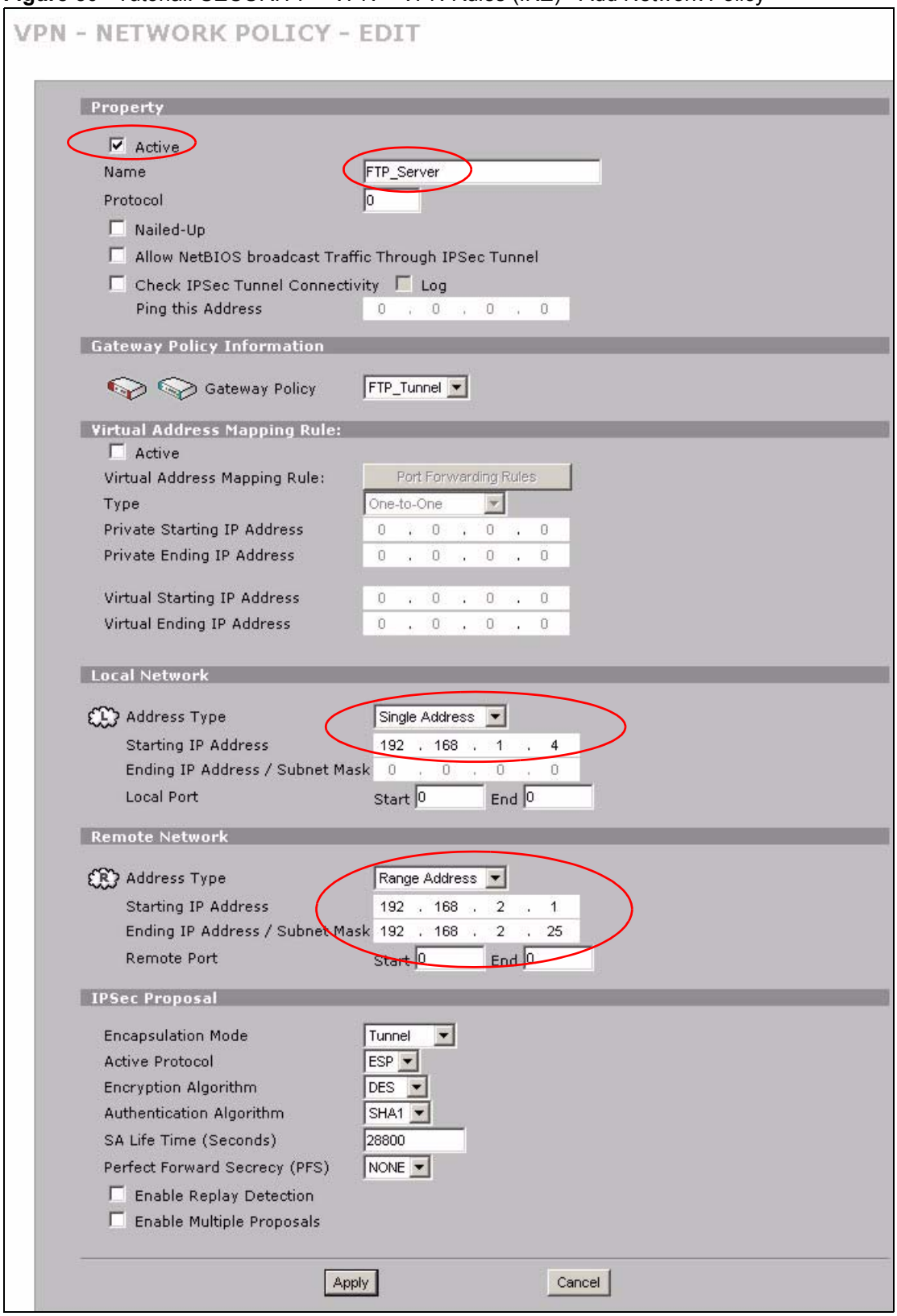
Figure 49 Tutorial: SECURITY > VPN > VPN Rules (IKE): With Gateway Policy Example



4 Use this screen to specify which computers behind the routers can use the VPN tunnel. Configure the fields that are circled as follows and click **Apply**. You may notice that the example does not specify the port numbers. This is due to the following reasons.

- While FTP uses a control session on port 20, the port for the data session is not fixed. So this example uses the firewall's FTP application layer gateway (ALG) to handle this instead of specifying port numbers in this VPN network policy.
- The firewall provides better security because it operates at layer 4 and checks traffic sessions. The VPN network policy only operates at layer 3 and just checks IP addresses and port numbers.

Figure 50 Tutorial: SECURITY > VPN > VPN Rules (IKE)> Add Network Policy



4.3.2 Configuring the Firewall Rules

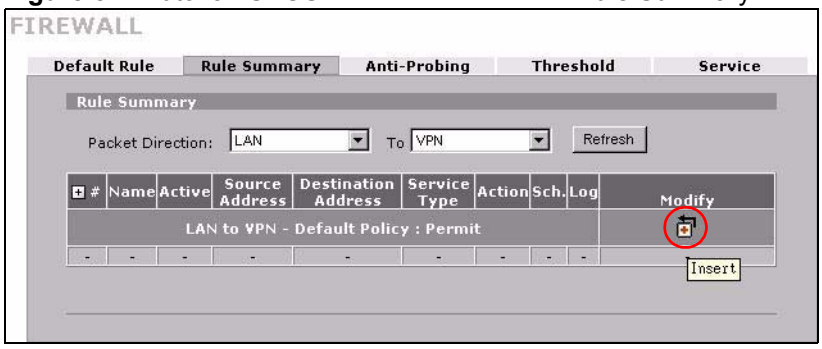
Suppose you only want FTP traffic to go to the FTP server, so you want to block all other traffic types (like chat, e-mail, web and so on). The following sections show how to configure firewall rules to enforce these restrictions.

4.3.2.1 Firewall Rule to Allow Access Example

Configure a firewall rule that allows FTP access from the VPN tunnel to the FTP server.

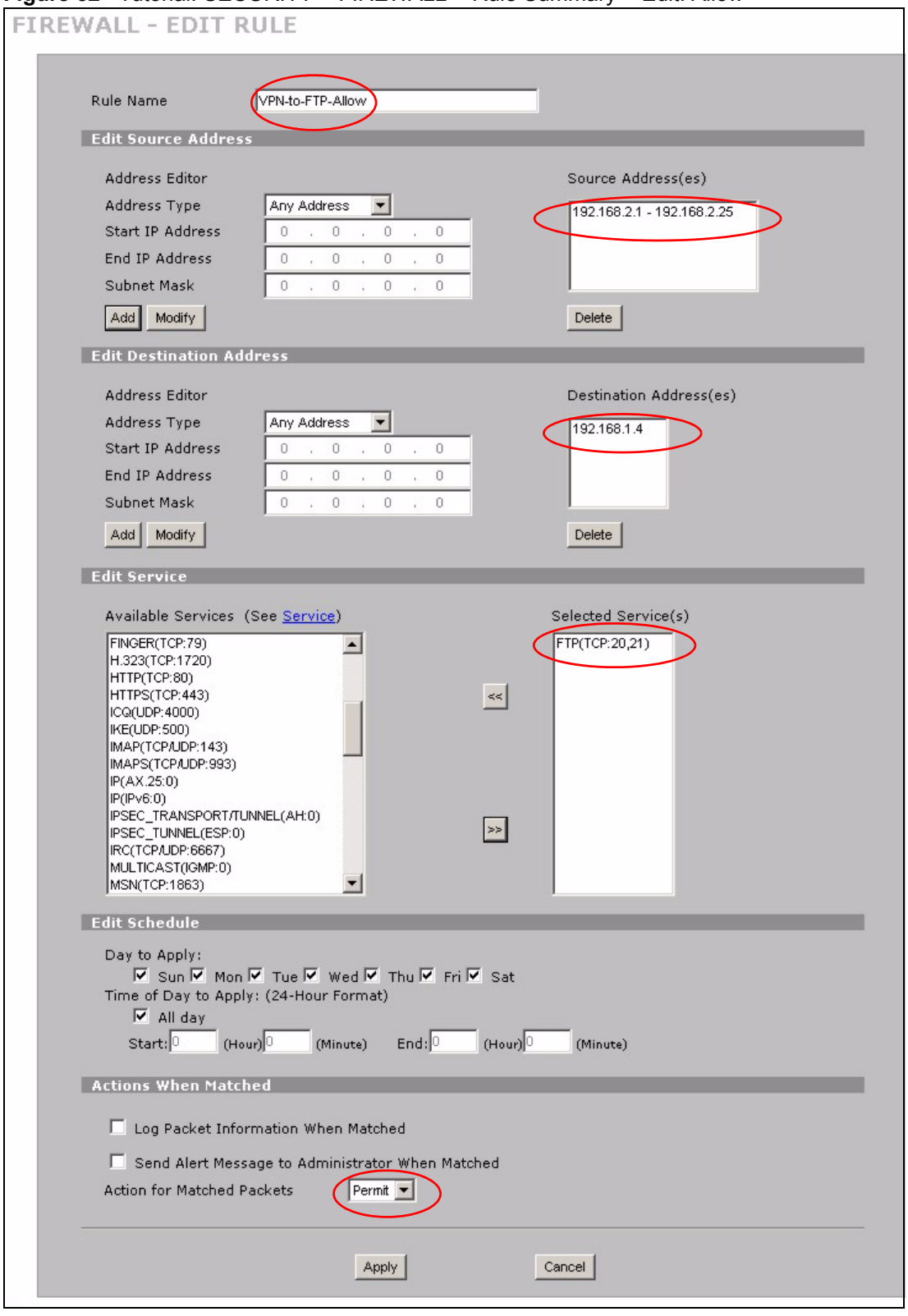
1. Click **Security > Firewall > Rule Summary**.
2. Select **VPN To LAN** as the packet direction and click **Refresh**.
3. Click the insert icon at the top of the **Modify** column.

Figure 51 Tutorial: SECURITY > FIREWALL > Rule Summary



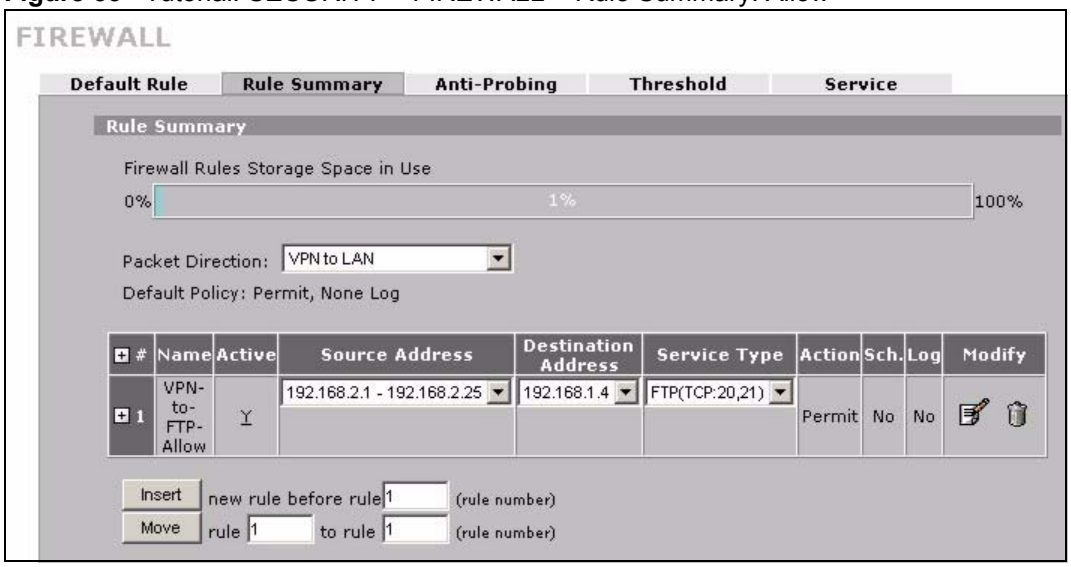
4. Configure the rule as follows and click **Apply**. The source addresses are the VPN rule's remote network and the destination address is the LAN FTP server.

Figure 52 Tutorial: SECURITY > FIREWALL > Rule Summary > Edit: Allow



5 The rule displays in the summary list of VPN to LAN firewall rules.

Figure 53 Tutorial: SECURITY > FIREWALL > Rule Summary: Allow

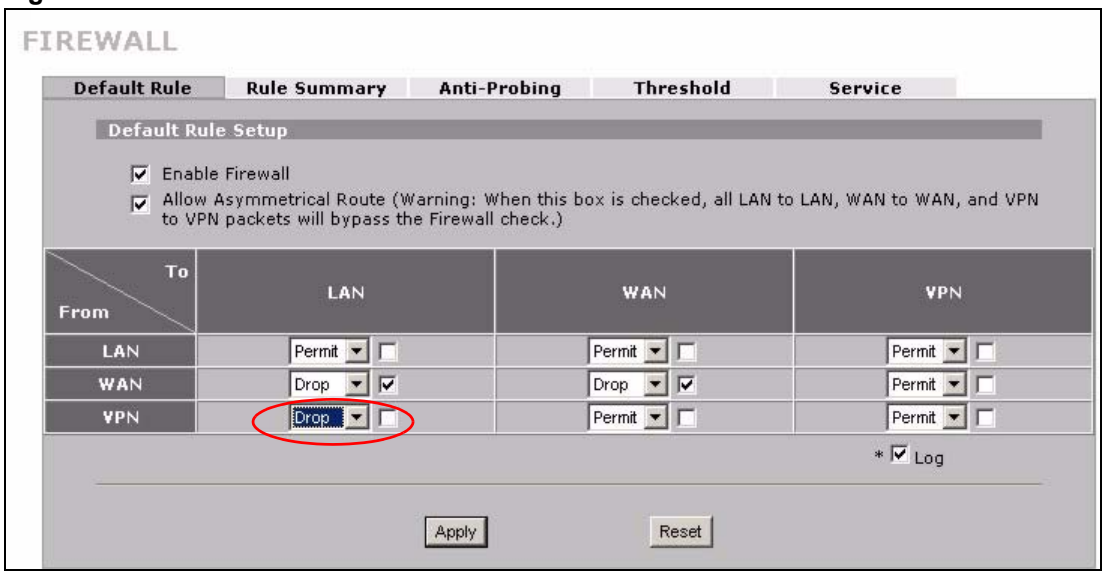


4.3.2.2 Default Firewall Rule to Block Other Access Example

Now you configure the default firewall rule to block all VPN to LAN traffic. This blocks any other types of access from the VPN tunnels to the LAN FTP server. This means that you need to configure more firewall rules if you want to allow any other VPN access to the LAN.

1. Click **SECURITY > FIREWALL > Default Rule**.
2. Configure the screen as follows and click **Apply**.

Figure 54 Tutorial: SECURITY > FIREWALL > Default Rule: Block From VPN To LAN



5

Registration

5.1 myZyXEL.com overview

myZyXEL.com is ZyXEL's online services center where you can register your ZyWALL and manage subscription services available for the ZyWALL.

You need to create an account before you can register your device and activate the services at myZyXEL.com.

You can directly create a myZyXEL.com account, register your ZyWALL and activate a service using the **REGISTRATION** screen. Alternatively, go to http://www.myZyXEL.com with the ZyWALL's serial number and LAN MAC address to register it. Refer to the web site's on-line help for details.

To activate a service on a ZyWALL, you need to access myZyXEL.com via that ZyWALL.

5.1.1 Subscription Services Available on the ZyWALL

At the time of writing, the ZyWALL can use anti-virus and IDP (Intrusion Detection and Prevention) subscription services.

Anti-virus allows the ZyWALL to scan packets for computer viruses and deletes the infected packets.

IDP allows the ZyWALL to detect malicious or suspicious packets and respond immediately.

The ID&P and anti-virus features use the same signature files on the ZyWALL to detect and scan for viruses. After the service is activated, the ZyWALL downloads the up-to-date signature files from the update server (http://myupdate.zywall.zyxel.com).

You will get automatic e-mail notification of new signature releases from mySecurityZone after you activate the IDP/Anti-virus service. You can also check for new signature or virus updates at http://mysecurity.zyxel.com.

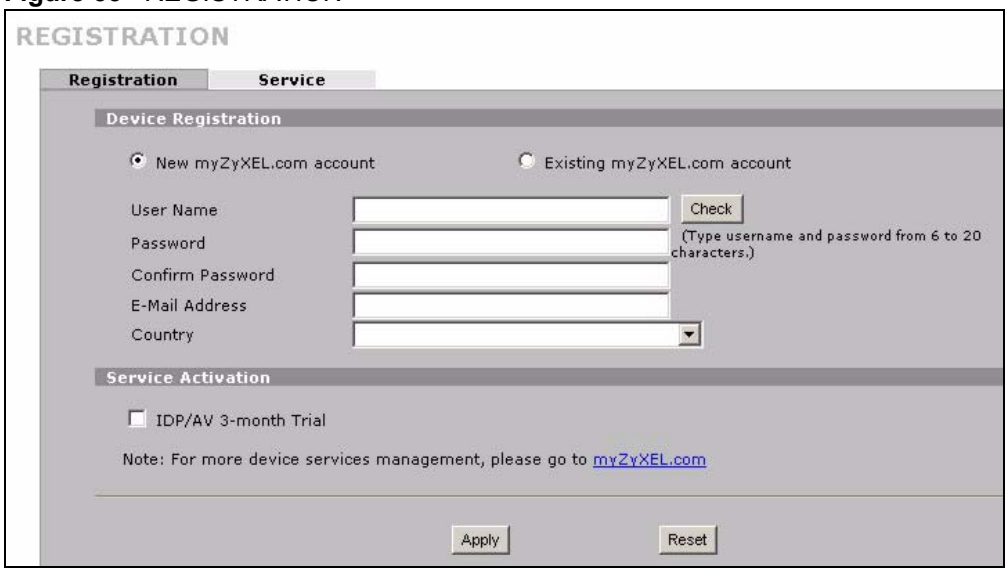
See the chapters about anti-virus and IDP for more information.

To update the signature file or use a subscription service, you have to register and activate the corresponding service at myZyXEL.com (through the ZyWALL).

5.2 Registration

To register your ZyWALL with myZyXEL.com and activate a service, such as anti-virus, click **REGISTRATION** in the navigation panel to open the screen as shown next.

Figure 55 REGISTRATION



If the ZyWALL is registered already, this screen is read-only and indicates whether trial services are activated. Use the **Service** screen to update your service subscription status.

Figure 56 REGISTRATION: Registered Device

The following table describes the labels in this screen.

Table 22 REGISTRATION

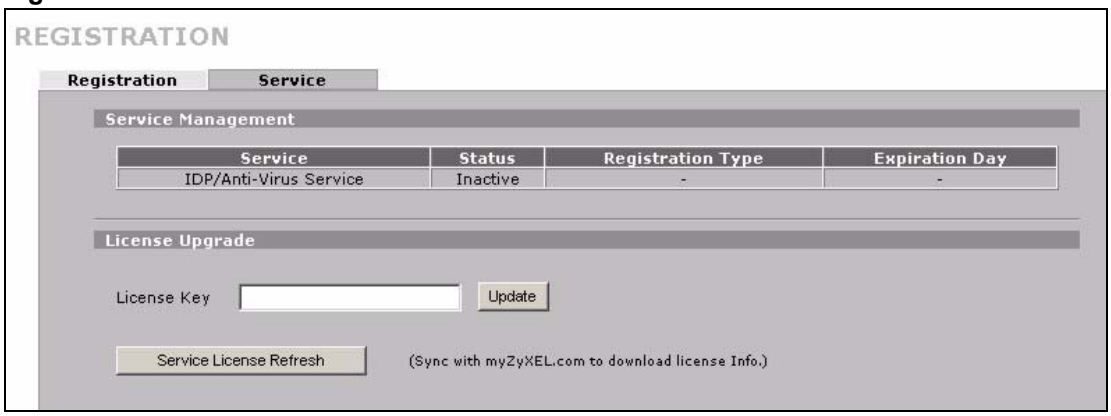
LABEL	DESCRIPTION
Device Registration	If you select **Existing myZyXEL.com account**, only the **User Name** and **Password** fields are available.
New myZyXEL.com account	If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your ZyWALL.
Existing myZyXEL.com account	If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your ZyWALL.
User Name	Enter a user name for your myZyXEL.com account. The name should be from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Check	Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used.
Password	Enter a password of between six and 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Confirm Password	Enter the password again for confirmation.
E-Mail Address	Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces.
Country	Select your country from the drop-down box list.
Service Activation	You can try trial service subscription. After the trial expires, you can buy an iCard and enter the license key in the **REGISTRATION Service** screen to extend the service.
IDP/AV 3-month Trial	Select the check box to activate a trial. The trial period starts the day you activate the trial.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

5.3 Service

After you activate a trial, you can also use the **Service** screen to register and enter your iCard's PIN number (license key). Click **REGISTRATION** > **Service** to open the screen as shown next.

If you restore the ZyWALL to the default configuration file or upload a different configuration file after you register, click the **Service License Refresh** button to update license information.

Figure 57 REGISTRATION > Service



The following table describes the labels in this screen.

Table 23 REGISTRATION > Service

LABEL	DESCRIPTION
Service Management	
Service	This field displays the service name available on the ZyWALL.
Status	This field displays whether a service is activated (**Active**) or not (**Inactive**).
Registration Type	This field displays whether you applied for a trial application (**Trial**) or registered a service with your iCard's PIN number (**Standard**).
Expiration Day	This field displays the date your service expires.
License Upgrade	
License Key	Enter your iCard's PIN number and click **Update** to activate or extend a standard service subscription. If a standard service subscription runs out, you need to buy a new iCard (specific to your ZyWALL) and enter the new PIN number to extend the service.
Service License Refresh	Click this button to renew service license information (such as the license key, registration status and expiration day).

PART II
Network

LAN Screens (107)
Bridge Screens (119)
WAN Screens (125)

6

LAN Screens

This chapter describes how to configure LAN settings. This chapter is not applicable when the ZyWALL is in bridge mode.

6.1 LAN, WAN and the ZyWALL

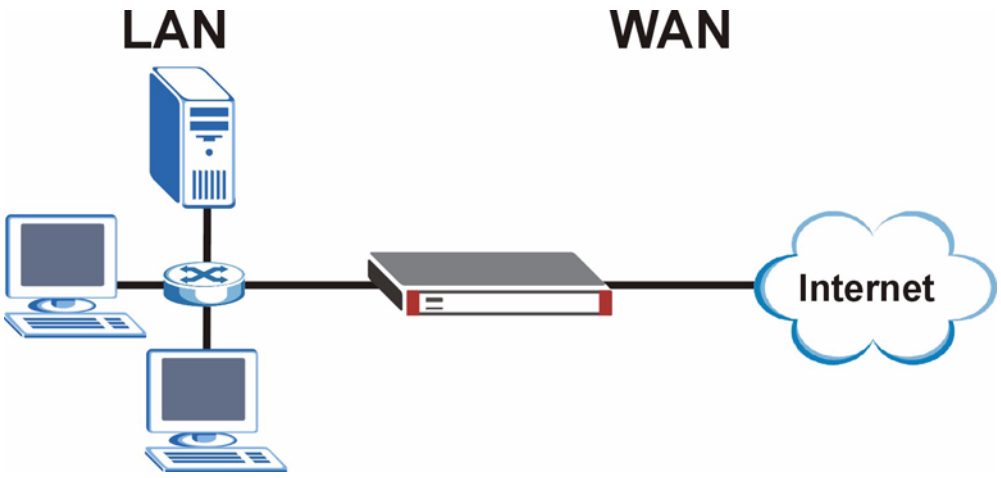
A network is a shared communication system to which many computers are attached.

The Local Area Network (LAN) includes the computers and networking devices in your home or office that you connect to the ZyWALL's LAN ports.

The Wide Area Network (WAN) is another network (most likely the Internet) that you connect to the ZyWALL's WAN port. See Chapter 8 on page 125 for how to use the WAN screens to set up your WAN connection.

The LAN and the WAN are two separate networks. The ZyWALL controls the traffic that goes between them. The following graphic gives an example.

Figure 58 LAN and WAN



6.2 DHCP

The ZyWALL can use DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) to automatically assign IP addresses subnet masks, gateways, and some network information like the IP addresses of DNS servers to the computers on your LAN. You can alternatively have the ZyWALL relay DHCP information from another DHCP server. If you disable the ZyWALL's DHCP service, you must have another DHCP server on your LAN, or else the computers must be manually configured.

6.2.1 IP Pool Setup

The ZyWALL is pre-configured with a pool of IP addresses for the computers on your LAN. See Appendix A on page 425 for the default IP pool range. Do not assign your LAN computers static IP addresses that are in the DHCP pool.

6.3 RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

RIP Version controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and **RIP Version** to **RIP-1**.

6.4 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address

224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyWALL queries all directly connected networks to gather group membership. After that, the ZyWALL periodically updates this information. IP multicasting can be enabled/disabled on the ZyWALL LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

6.5 WINS

WINS (Windows Internet Naming Service) is a Windows implementation of NetBIOS Name Server (NBNS) on Windows. It keeps track of NetBIOS computer names. It stores a mapping table of your network's computer names and IP addresses. The table is dynamically updated for IP addresses assigned by DHCP. This helps reduce broadcast traffic since computers can query the server instead of broadcasting a request for a computer name's IP address. In this way WINS is similar to DNS, although WINS does not use a hierarchy (unlike DNS). A network can have more than one WINS server. Samba can also serve as a WINS server.

6.6 DNS Overview

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

The ZyWALL can get addresses of DNS servers in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the ZyWALL's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
3. You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see Section 6.7.1 on page 110).

6.7 DNS Servers

There are three places where you can configure DNS setup on the ZyWALL.

1. Use the **MAINTENANCE > General** screen to configure the ZyWALL to use a DNS server to resolve domain names for ZyWALL system features like VPN, DDNS and the time server.
2. Use the **NETWORK > LAN** screen to configure the DNS server information that the ZyWALL sends to the DHCP client devices on the LAN.

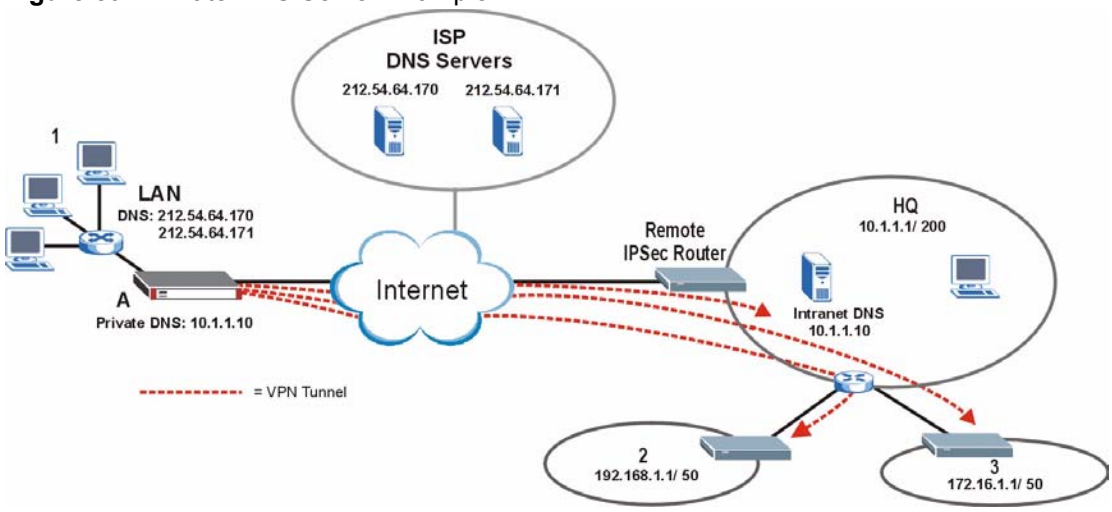
3 Use the **ADVANCED > REMOTE MGMT DNS** screen to configure the ZyWALL (in router or zero configuration mode) to accept or discard DNS queries.

6.7.1 Private DNS Server Behind a Remote IPSec Router

In cases where you want to use domain names to access Intranet servers on a remote private network that has a private DNS server, you must identify that DNS server. You cannot use DNS servers on your ZyWALL's LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote private network.

The following figure depicts an example where three VPN tunnels are created from ZyWALL A; one to branch office **2**, one to branch office **3** and another to headquarters (**HQ**). In order to access computers that use private domain names on the **HQ** network, the ZyWALL at branch office **1** uses the Intranet DNS server in headquarters.

Figure 59 Private DNS Server Example

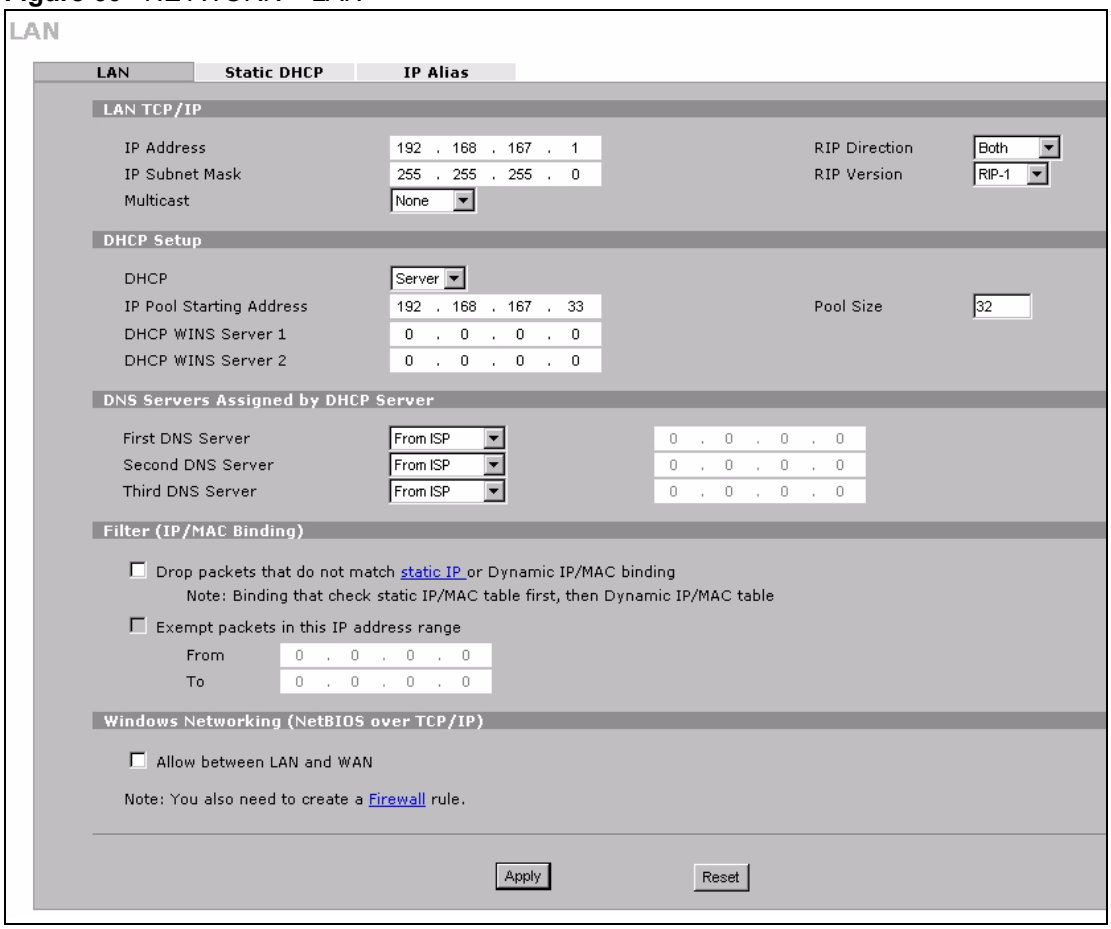


If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote private network.

6.8 LAN

Click **NETWORK** > **LAN** to open the **LAN** screen. Use this screen to configure the ZyWALL's IP address and other LAN TCP/IP settings as well as the built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

Figure 60 NETWORK > LAN



The following table describes the labels in this screen.

Table 24 NETWORK > LAN

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Type the IP address of your ZyWALL in dotted decimal notation. 192.168.167.1 is the factory default. Alternatively, click the right mouse button to copy and/or paste the IP address. See Appendix C on page 455 for details about IP addresses.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyWALL automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. See Appendix C on page 455 for details about IP subnetting.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. **Both** is the default.

Table 24 NETWORK > LAN (continued)

LABEL	DESCRIPTION
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*.
DHCP Setup	
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to **Server**. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. When set as a server, fill in the **IP Pool Starting Address** and **Pool Size** fields. Select **None** to stop the ZyWALL from acting as a DHCP server. When you select **None**, you must have another DHCP server on your LAN, or else the computers must be manually configured.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DHCP Server Address	Type the IP address of the DHCP server to which you want the ZyWALL to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
DHCP WINS Server 1, 2	Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
DNS Servers Assigned by DHCP Server	The ZyWALL passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP client. The ZyWALL only passes this information to the LAN DHCP client when you have selected **Server** from the **DHCP** dropdown box. When **None** is selected, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must have their DNS server addresses manually configured.

Table 24 NETWORK > LAN (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the ZyWALL's WAN IP address). Use the drop-down list box to select a DNS server IP address that the ISP assigns in the field to the right. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the ZyWALL act as a DNS proxy. The ZyWALL's LAN IP address displays in the field to the right (read-only). The ZyWALL tells the DHCP client on the LAN that the ZyWALL itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyWALL, the ZyWALL forwards the query to the ZyWALL's system DNS server (configured in the **DNS System** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Filter (IP/MAC Binding	
Drop packets that do not match static IP or Dynamic IP/MAC binding	Select this to allow traffic only from devices on the LAN which have received an IP address from the ZyWALL. This is done by allowing traffic only from devices on the LAN with specific combinations of IP and MAC addresses. These IP addresses are dynamically assigned by the ZyWALL or manually set using static DHCP. See the **Static DHCP** screen for a list of static IP/MAC address combinations. See the **DHCP Table** available from the **Home** screen for a list of dynamically assigned IP/MAC address combinations.
Exempt packets in this IP address range.	Set the ZyWALL to allow packets from the LAN with source IP addresses within a specified range. This allows packets even when their IP and MAC addresses do not match those specified in the **Static DHCP** screen or **DHCP Table**. Type this range of IP addresses in the **From** and **To** fields.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN port and from the WAN port to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN port to the WAN port and from the WAN port to the LAN port.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

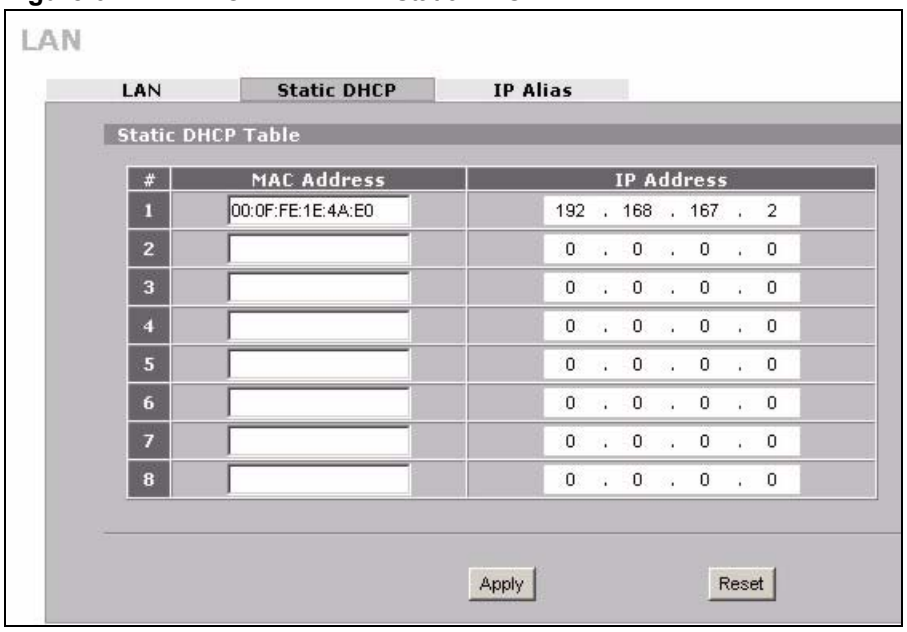
6.9 LAN Static DHCP

This table allows you to assign an IP address on the LAN to a specific individual computer based on its MAC address.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your ZyWALL's static DHCP settings, click **NETWORK** > **LAN** > **Static DHCP**. The screen appears as shown.

Figure 61 NETWORK > LAN > Static DHCP



The following table describes the labels in this screen.

Table 25 NETWORK > LAN > Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address of a computer on your LAN.
IP Address	Type the IP address that you want to assign to the computer on your LAN. Alternatively, click the right mouse button to copy and/or paste the IP address.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.10 LAN IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface.

The ZyWALL supports three logical LAN interfaces via its single physical LAN Ethernet interface. The ZyWALL itself is the gateway for each of the logical LAN networks.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

Make sure that the subnets of the logical networks do not overlap.

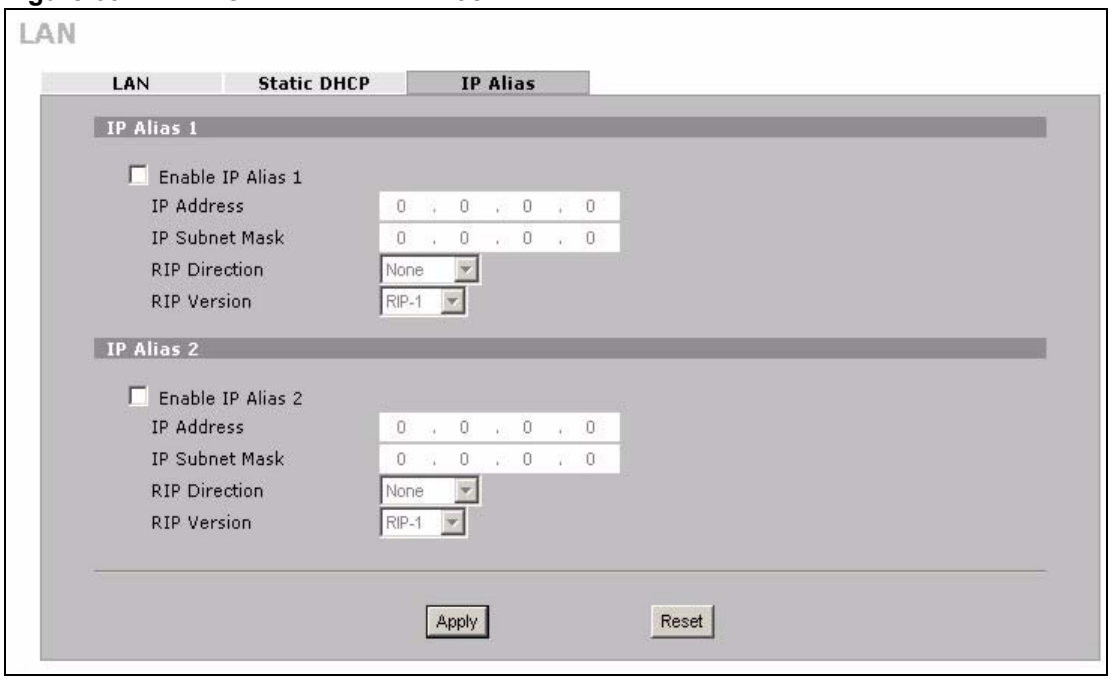
The following figure shows a LAN divided into subnets A, B, and C.

Figure 62 Physical Network and Partitioned Logical Networks

The ZyWALL must be in router mode in order to use IP alias.

To change your ZyWALL's IP alias settings, click **NETWORK** > **LAN** > **IP Alias**. The screen appears as shown.

Figure 63 NETWORK > LAN > IP Alias



The following table describes the labels in this screen.

Table 26 NETWORK > LAN > IP Alias

LABEL	DESCRIPTION
Enable IP Alias 1, 2	Select the check box to configure another LAN network for the ZyWALL.
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.

Table 26 NETWORK > LAN > IP Alias

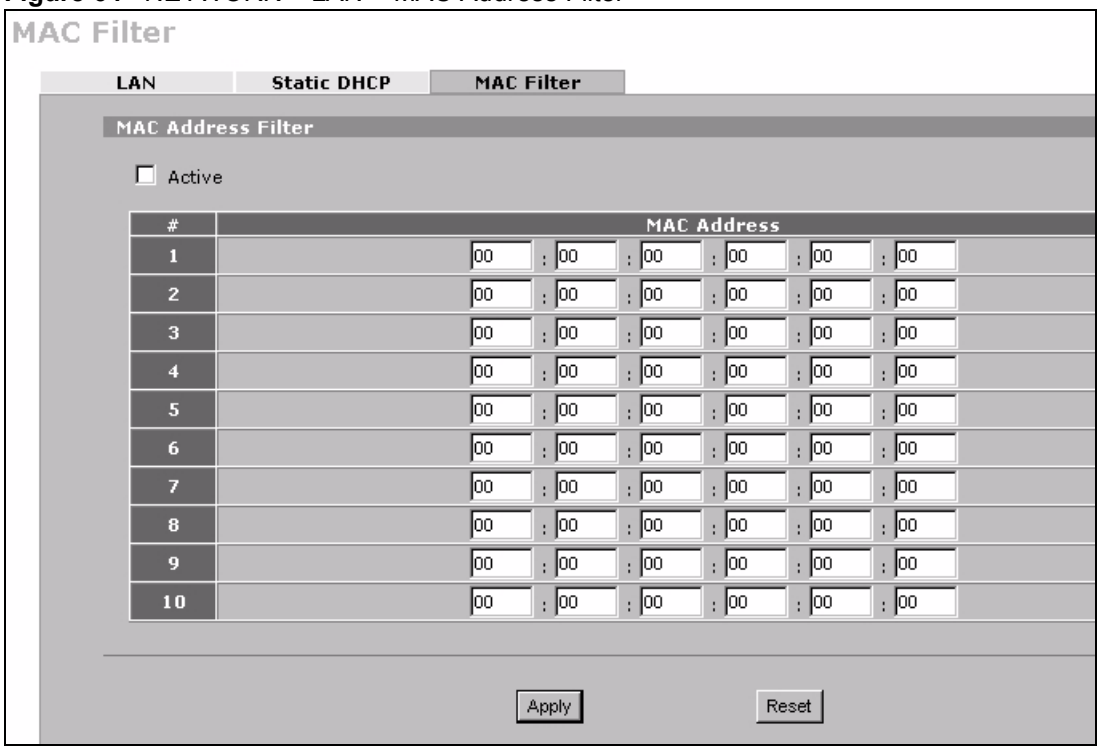
LABEL	DESCRIPTION
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.11 MAC Filter

The MAC filter screen allows you to limit access to specific devices when the ZyWALL is in zero configuration mode. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

To change your ZyWALL's MAC filter settings, click the **NETWORK** > **LAN** > **MAC Filter**. The screen appears as shown.

Figure 64 NETWORK > LAN > MAC Address Filter



The following table describes the labels in this menu.

Table 27 NETWORK > LAN > MAC Address Filter

LABEL	DESCRIPTION
Active	Select or clear the check box to enable or disable MAC address filtering. Enable MAC address filtering to only give access to computers with a MAC address that matches an entry in the list. Disable MAC address filtering to have the router not perform MAC filtering.
#	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the allowed that are allowed or denied access to the ZyWALL in these address fields.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

7

Bridge Screens

This chapter describes how to configure bridge settings. This chapter is only applicable when the ZyWALL is in bridge mode (see Section 24.11 on page 385 for how to turn on bridge mode).

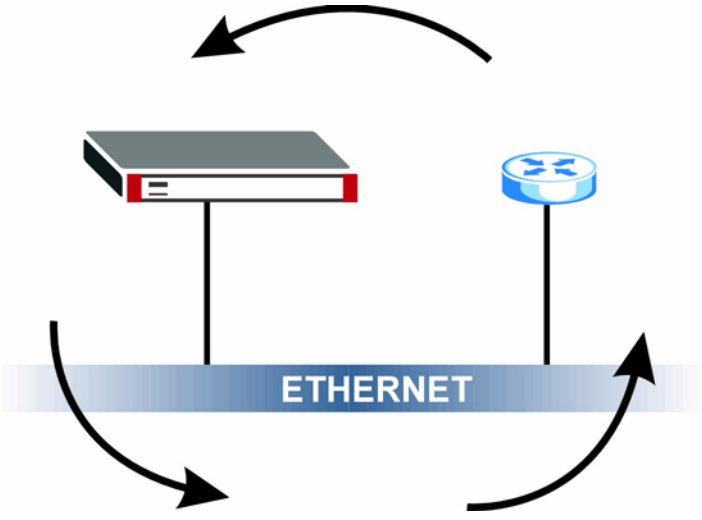
7.1 Bridge Loop

The ZyWALL can act as a bridge between a switch and a wired LAN or between two routers.

Be careful to avoid bridge loops when you enable bridging in the ZyWALL. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following example shows the network topology that can lead to this problem:

- If your ZyWALL (in bridge mode) is connected to a wired LAN while communicating with another bridge or a switch that is also connected to the same wired LAN as shown next.

Figure 65 Bridge Loop: Bridge Connected to Wired LAN



To prevent bridge loops, ensure that your ZyWALL is not set to bridge mode while connected to two wired segments of the same LAN or you enable RSTP in the **Bridge** screen.

This chapter introduces the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

7.2 Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other STP-compliant bridges in your network to ensure that only one route exists between any two stations on the network.

7.2.1 Rapid STP (RSTP)

The ZyWALL uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) to allow faster convergence of the spanning tree (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge that then notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

In this user's guide, "STP" refers to both STP and RSTP.

7.2.2 STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame from the root bridge to that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the next table.

Table 28 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this bridge has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

7.2.3 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware bridges exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

7.2.4 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 29 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

7.3 Bridge

Select **Bridge** and click **Apply** in the **MAINTENANCE > Device Mode** screen to have the ZyWALL function as a bridge.

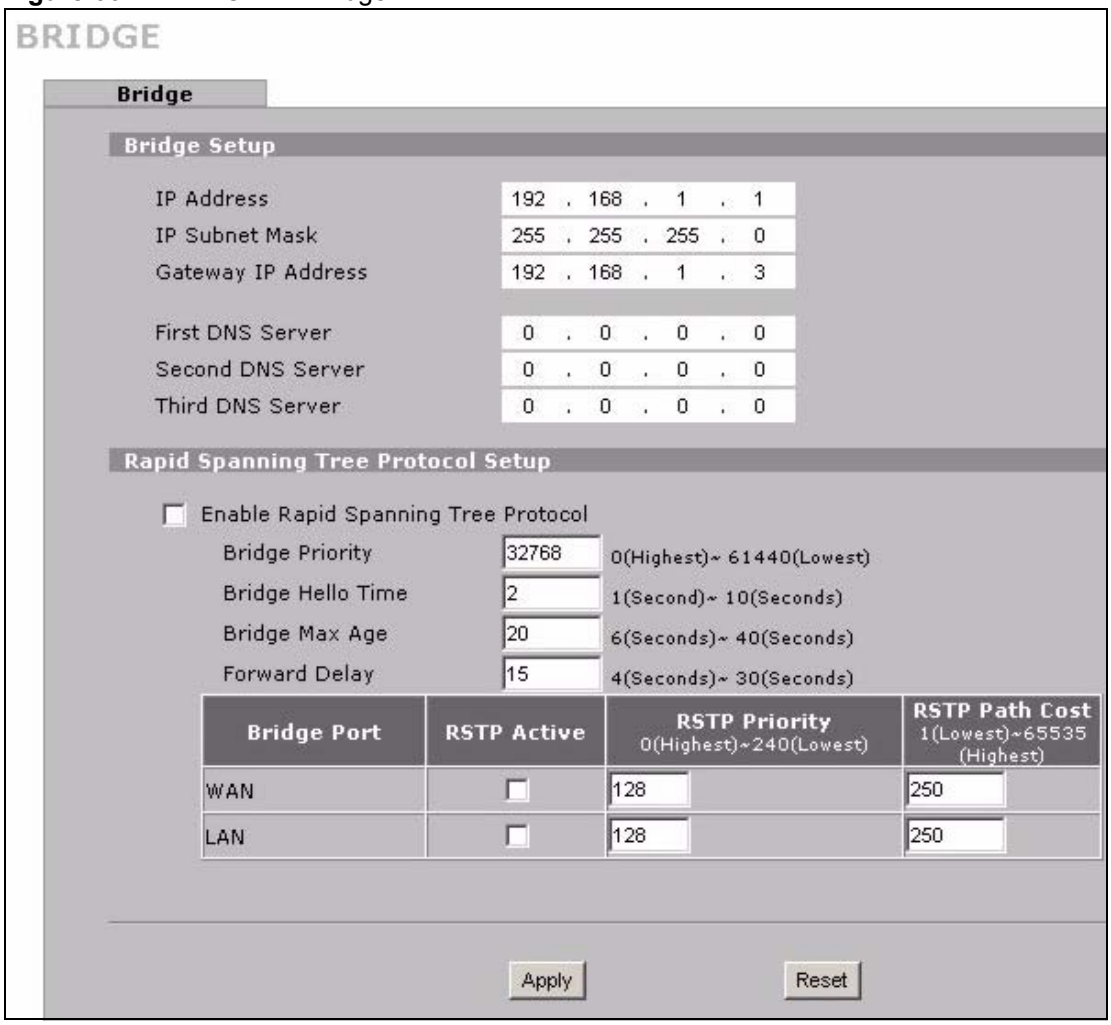
In bridge mode, the ZyWALL functions as a transparent firewall (also known as a bridge firewall). The ZyWALL bridges traffic traveling between the ZyWALL's interfaces and still filters and inspects packets. You do not need to change the configuration of your existing network.

You can use the firewall and VPN in bridge mode. See the user’s guide for a list of other features that are available in bridge mode.

Click **NETWORK** > **BRIDGE** to display the screen shown next. Use this screen to configure bridge and RSTP (Rapid Spanning Tree Protocol) settings.

In bridge mode, if you need to let DHCP clients behind the ZyWALL use a DHCP server on the WAN, enable the default WAN to LAN firewall rule for the **BOOTP_CLIENT** service.

Figure 66 NETWORK > Bridge


BRIDGE
Bridge
Bridge Setup
IP Address 192 . 168 . 1 . 1
IP Subnet Mask 255 . 255 . 255 . 0
Gateway IP Address 192 . 168 . 1 . 3
First DNS Server 0 . 0 . 0 . 0
Second DNS Server 0 . 0 . 0 . 0
Third DNS Server 0 . 0 . 0 . 0
Rapid Spanning Tree Protocol Setup
Enable Rapid Spanning Tree Protocol
Bridge Priority 32768 0(Highest)~ 61440(Lowest)
Bridge Hello Time 2 1(Second)~ 10(Seconds)
Bridge Max Age 20 6(Seconds)~ 40(Seconds)
Forward Delay 15 4(Seconds)~ 30(Seconds)
Bridge Port
RSTP Active
RSTP Priority 0(Highest)~240(Lowest)
RSTP Path Cost 1(Lowest)~65535 (Highest)
WAN 128 250
LAN 128 250
Apply
Reset

The following table describes the labels in this screen.

Table 30 NETWORK > Bridge

LABEL	DESCRIPTION
Bridge Setup	
IP Address	Type the IP address of your ZyWALL in dotted decimal notation. Use an IP address in the same subnet as the network to which you connect the ZyWALL. Make sure the IP address does not conflict with any other device on the network.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.
Gateway IP Address	Enter the gateway IP address.

Table 30 NETWORK > Bridge (continued)

LABEL	DESCRIPTION
First/Second/Third DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The ZyWALL uses the DNS server (in the order you specify here) to resolve domain names for things like the time server. Enter the DNS server IP address(es) in the field(s) to the right.
Rapid Spanning Tree Protocol Setup	
Enable Rapid Spanning Tree Protocol	Select the check box to activate RSTP on the ZyWALL.
Bridge Priority	Enter a number between 0 and 61440 as bridge priority of the ZyWALL. Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the root. If multiple devices have the lowest priority, the device with the lowest MAC address becomes the root. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forward Delay.
Bridge Hello Time	Enter an interval (between 1 and 10) in seconds that the root bridge waits before sending a hello packet.
Bridge Max Age	Enter an interval (between 6 and 40) in seconds that a bridge waits to get a Hello BPDU from the root bridge.
Forward Delay	Enter the length of time (between 4 and 30) in seconds that a bridge remains in the listening and learning port states. The default is 15 seconds.
Bridge Port	This is the bridge port type.
RSTP Active	Select the check box to enable RSTP on the corresponding port.
RSTP Priority 0(Highest)~240(Lowest)	Enter a number between 0 and 240 as RSTP priority for the corresponding port. 0 is the highest.
RSTP Path Cost 1(Lowest)~65535(Highest)	Enter a number between 1 and 65535 as RSTP path cost for the corresponding port. 65535 is the highest.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8

WAN Screens

This chapter describes how to configure WAN settings.

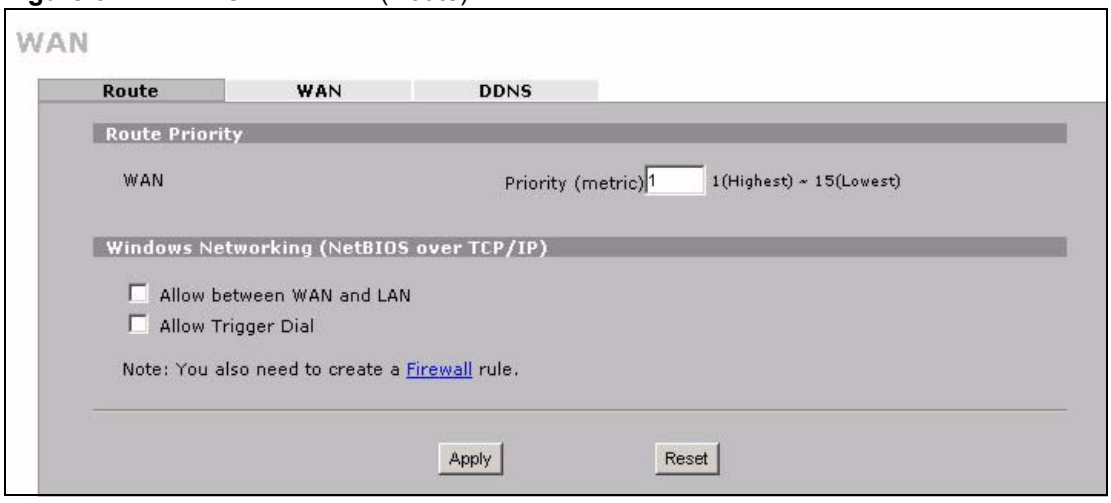
8.1 WAN Overview

- Use the **WAN Route** screen to configure route priority.
- Use the **WAN** screen to configure the WAN port for Internet access.
- Use the **DDNS** screen to configure your traffic redirect properties and parameters.

8.2 WAN Route

Click **NETWORK** > **WAN** to open the **Route** screen. Use this screen to configure the priorities of the ZyWALL's routes and settings for Windows Networking traffic.

Figure 67 NETWORK > WAN (Route)



The following table describes the labels in this screen.

Table 31 NETWORK > WAN (Route)

LABEL	DESCRIPTION
Route Priority	
WAN	Set the priority for the default WAN connection. Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Windows Networking (NetBIOS over TCP/IP):	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.
Allow between WAN and LAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8.3 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 32 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

8.4 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The ZyWALL can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the ZyWALL's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
3. You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see Section 6.7.1 on page 110).

8.5 WAN MAC Address

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

You can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file.

8.6 WAN

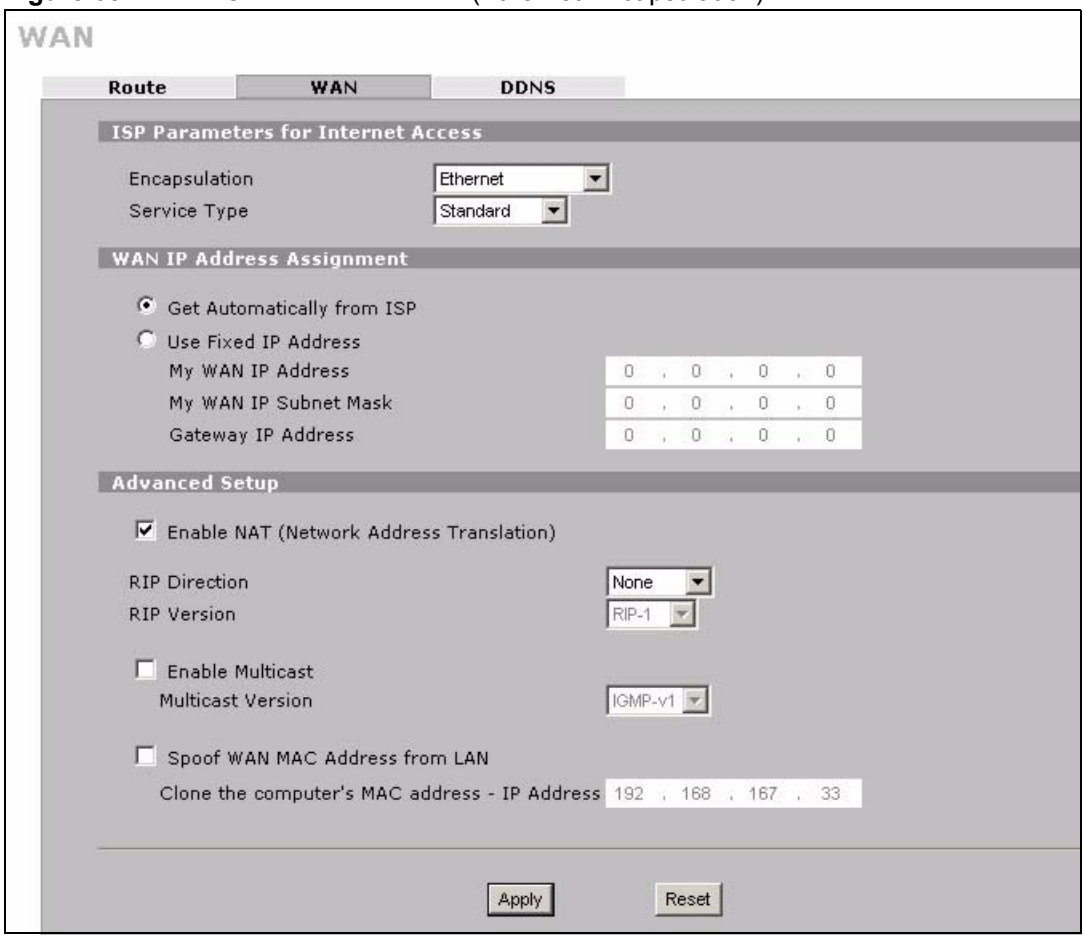
To change your ZyWALL's WAN ISP, IP and MAC settings, click **NETWORK** > **WAN** > **WAN**. The screen differs by the encapsulation.

8.6.1 WAN Ethernet Encapsulation

For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a **WAN-to-WAN/ZyWALL** firewall rule for those packets. Contact your ISP to find the correct port number.

The screen shown next is for **Ethernet** encapsulation.

Figure 68 NETWORK > WAN > WAN (Ethernet Encapsulation)



The following table describes the labels in this screen.

Table 33 NETWORK > WAN > WAN (Ethernet Encapsulation)

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from **Standard**, **Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**. The following fields do not appear with the **Standard** service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one. This field is not available for Telia Login.

Table 33 NETWORK > WAN > WAN (Ethernet Encapsulation) (continued)

LABEL	DESCRIPTION
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example login1.telia.com.
Relogin Every(min) (Telia Login only)	The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the ZyWALL to wait between logins.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
My WAN IP Subnet Mask	Enter the IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Gateway IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Advanced Setup	
Enable NAT (Network Address Translation)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select this check box to enable NAT.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **None**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives. When set to **None**, the ZyWALL will not send any RIP packets and will ignore any RIP packets received. By default, **RIP Direction** is set to **Both**.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.

Table 33 NETWORK > WAN > WAN (Ethernet Encapsulation) (continued)

LABEL	DESCRIPTION
Multicast Version	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Spoof WAN MAC Address	You can use the factory assigned default MAC Address or cloning the MAC address from a computer on your LAN. Otherwise, select the check box next to **Spoof WAN MAC Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Clone the computer's MAC address – IP Address	Enter the IP address of the computer on the LAN whose MAC you are cloning. It is recommended that you clone the MAC address prior to hooking up the WAN port.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8.6.2 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

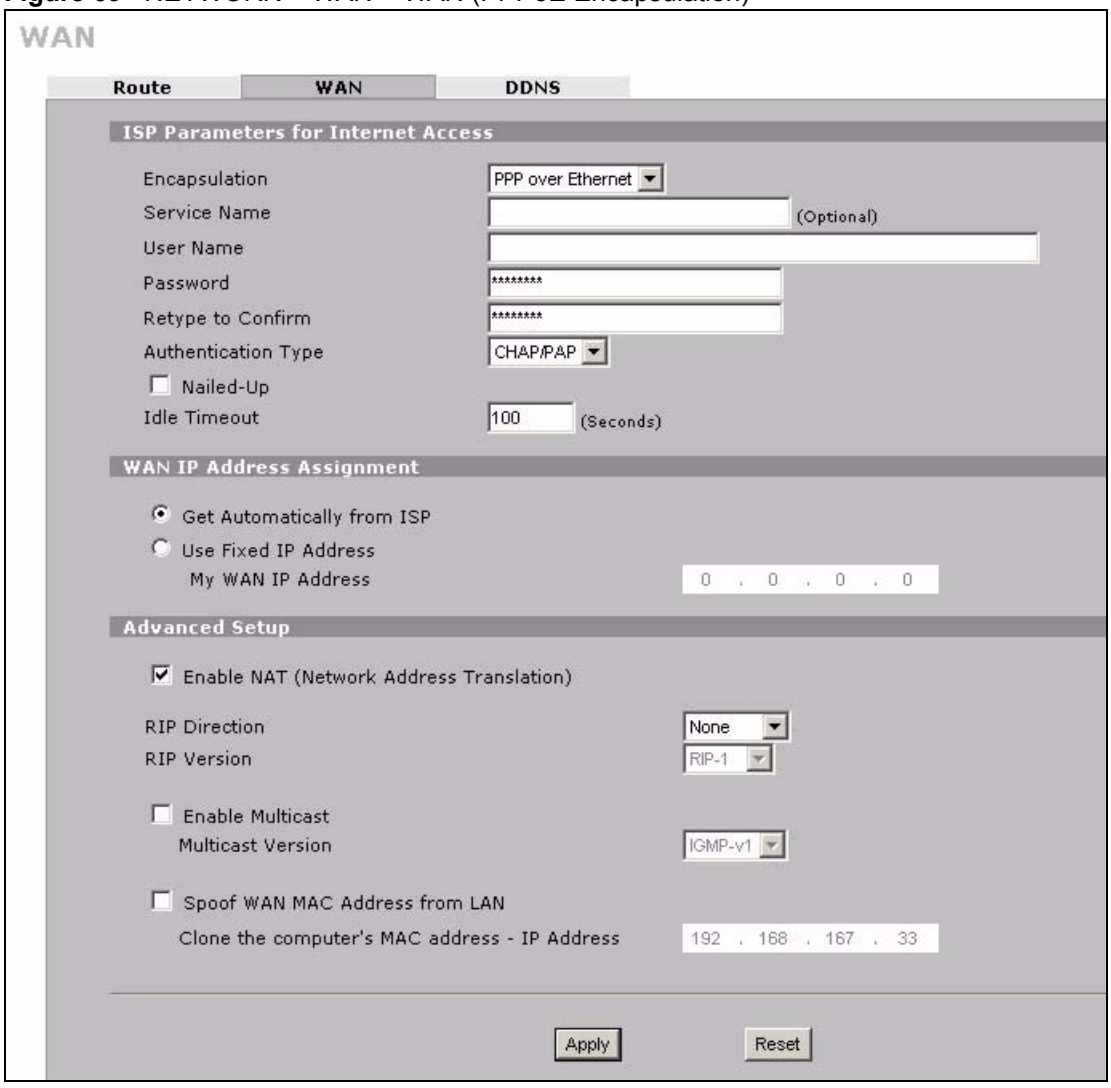
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyWALL (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyWALL does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

The screen shown next is for **PPPoE** encapsulation.

Figure 69 NETWORK > WAN > WAN (PPPoE Encapsulation)



The following table describes the labels in this screen.

Table 34 NETWORK > WAN > WAN (PPPoE Encapsulation)

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The PPPoE choice is for a dial-up connection using PPPoE.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.

Table 34 NETWORK > WAN > WAN (PPPoE Encapsulation) (continued)

LABEL	DESCRIPTION
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your ZyWALL accepts CHAP only. **PAP** - Your ZyWALL accepts PAP only.
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPPoE server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**
Advanced Setup	
Enable NAT (Network Address Translation)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select this checkbox to enable NAT. For more information about NAT see Chapter 16 on page 277.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **None**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives. When set to **None**, the ZyWALL will not send any RIP packets and will ignore any RIP packets received. By default, **RIP Direction** is set to **Both**.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.

Table 34 NETWORK > WAN > WAN (PPPoE Encapsulation) (continued)

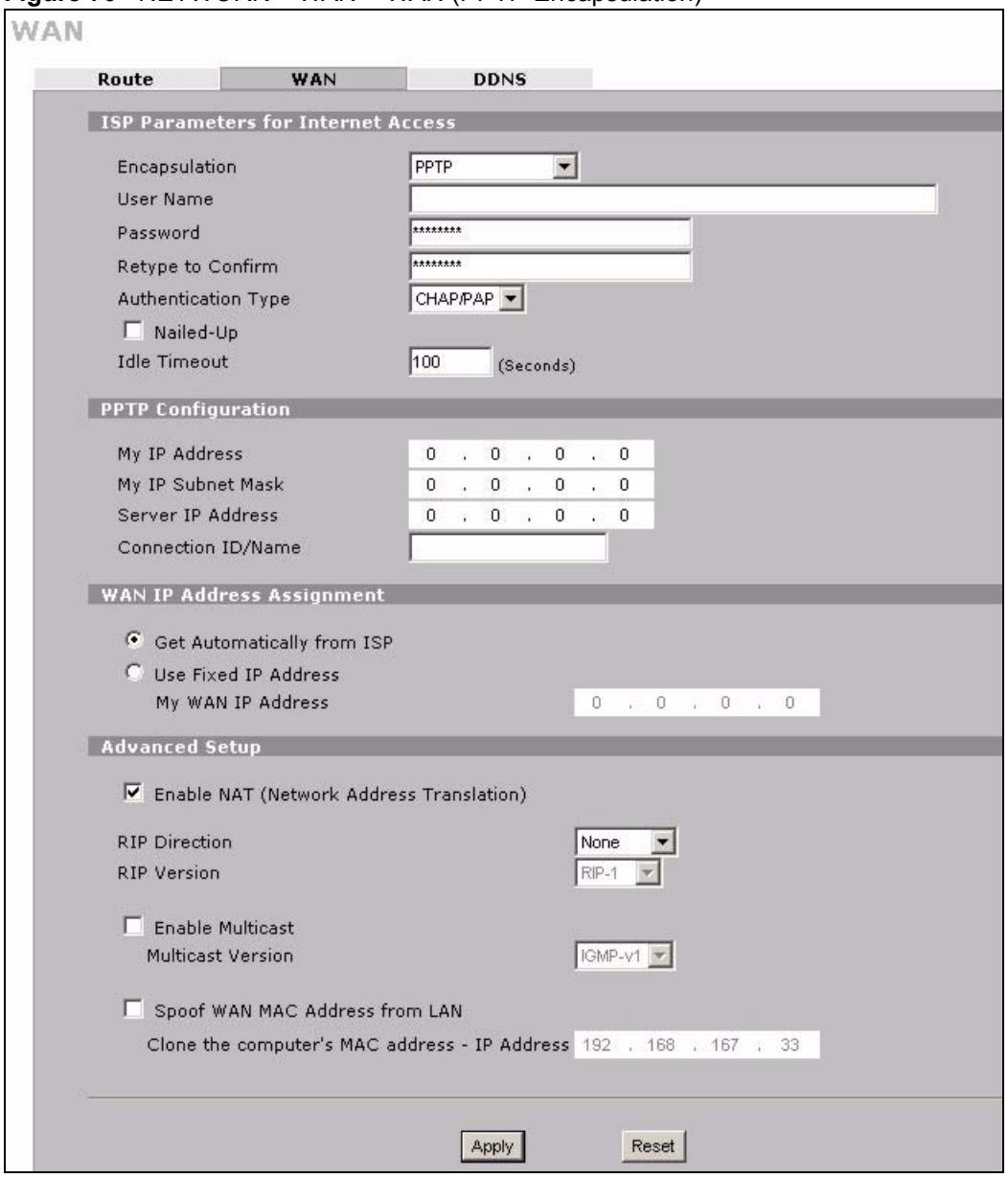
LABEL	DESCRIPTION
Multicast Version	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Spoof WAN MAC Address	You can use the factory assigned default MAC Address or cloning the MAC address from a computer on your LAN. Otherwise, select the check box next to **Spoof WAN MAC Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Clone the computer's MAC address – IP Address	Enter the IP address of the computer on the LAN whose MAC you are cloning. It is recommended that you clone the MAC address prior to hooking up the WAN port.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8.6.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The screen shown next is for **PPTP** encapsulation.

Figure 70 NETWORK > WAN > WAN (PPTP Encapsulation)



The following table describes the labels in this screen.

Table 35 NETWORK > WAN > WAN (PPTP Encapsulation)

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The ZyWALL supports only one PPTP server connection at any given time. You must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.

Table 35 NETWORK > WAN > WAN (PPTP Encapsulation) (continued)

LABEL	DESCRIPTION
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your ZyWALL accepts CHAP only. **PAP** - Your ZyWALL accepts PAP only.
Nailed-up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Type your identification name for the PPTP server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
Advanced Setup	
Enable NAT (Network Address Translation)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select this checkbox to enable NAT. For more information about NAT see Chapter 16 on page 277.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **None**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives. When set to **None**, the ZyWALL will not send any RIP packets and will ignore any RIP packets received. By default, **RIP Direction** is set to **Both**.

Table 35 NETWORK > WAN > WAN (PPTP Encapsulation) (continued)

LABEL	DESCRIPTION
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast Version	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Spoof WAN MAC Address	You can use the factory assigned default MAC Address or cloning the MAC address from a computer on your LAN. Otherwise, select the check box next to **Spoof WAN MAC Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Clone the computer's MAC address – IP Address	Enter the IP address of the computer on the LAN whose MAC you are cloning. It is recommended that you clone the MAC address prior to hooking up the WAN port.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

8.7 Dynamic DNS

Dynamic Domain Name System (Dynamic DNS or DDNS) allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

You must go to the Dynamic DNS service provider's website and register a user account and a domain name before you can use the Dynamic DNS service with your ZyWALL.

8.7.1 DYNDNS Wildcard

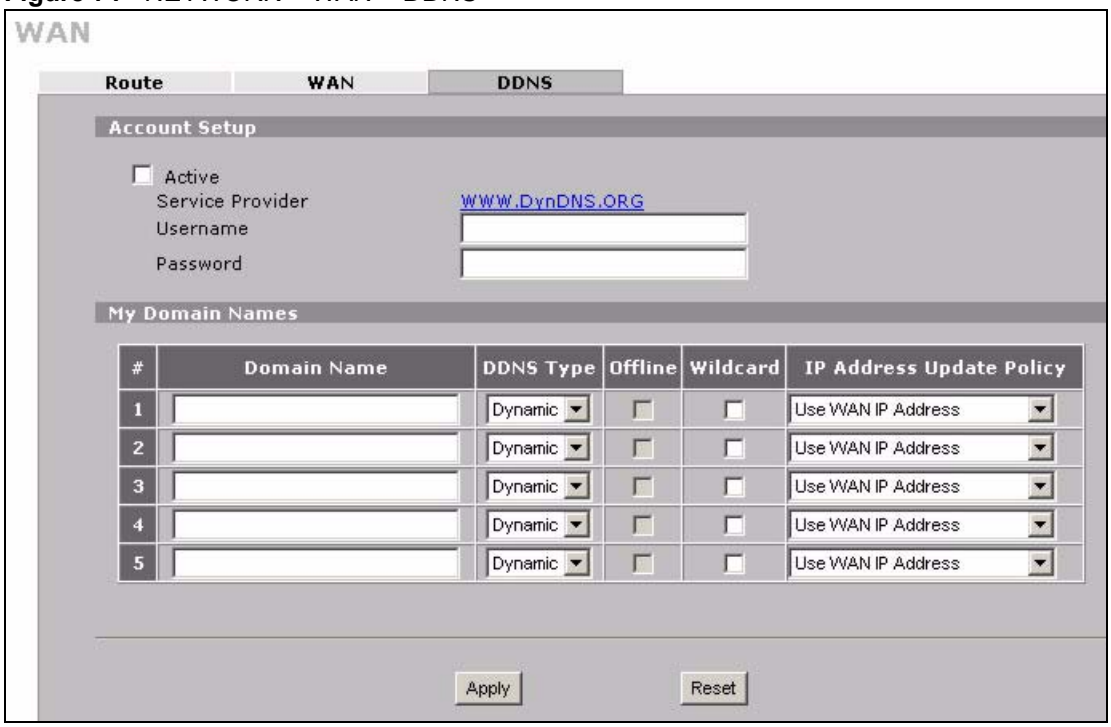
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

8.8 Configuring Dynamic DNS

To change your ZyWALL's DDNS, click **NETWORK** > **WAN** > **DDNS**. The screen appears as shown.

Figure 71 NETWORK > WAN > DDNS



The following table describes the labels in this screen.

Table 36 NETWORK > WAN > DDNS

LABEL	DESCRIPTION
Account Setup	
Active	Select this check box to use dynamic DNS.
Service Provider	Select the name of the Dynamic DNS service provider you use.
Username	Enter your user name. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
Password	Enter the password associated with the user name above. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
My Domain Names	
Domain Name 1~5	Enter the host names in these fields.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider. Select **Dynamic** if you have the Dynamic DNS service. Select **Static** if you have the Static DNS service. Select **Custom** if you have the Custom DNS service.
Offline	This option is available when **Custom** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Wildcard	Select the check box to enable DYNDNS Wildcard.
IP Address Update Policy	Select **Use WAN IP Address** to have the ZyWALL update the domain name with the WAN port's IP address. Select **Use User-Defined** and enter the IP address if you have a static IP address. Select **Let DDNS Server Auto Detect** only when there are one or more NAT routers between the ZyWALL and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

PART III
Security

Firewall (141)
Intrusion Detection and Prevention (IDP) (171)
Configuring IDP (175)
Anti-Virus (191)
IPSec VPN (203)
Certificates (243)
Authentication Server (271)

9

Firewall

This chapter shows you how to configure your ZyWALL's firewall.

9.1 Firewall Overview

In networking, the term "firewall" refers to a system or group of systems that enforces an access-control policy between two networks. It is generally a mechanism used to protect a trusted network from an untrusted network.

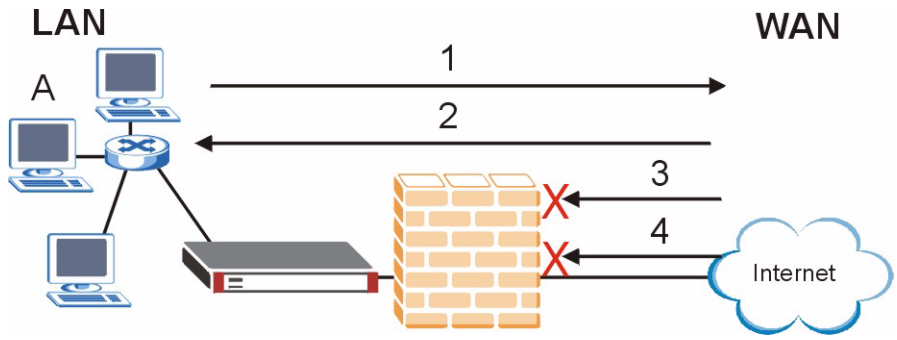
The ZyWALL physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks. The ZyWALL protects against Denial of Service (DoS) attacks, prevents theft, destruction and modification of data, and logs events.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.
- allows VPN traffic between the networks.

The following figure illustrates the default firewall action. User A can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 72 Default Firewall Action



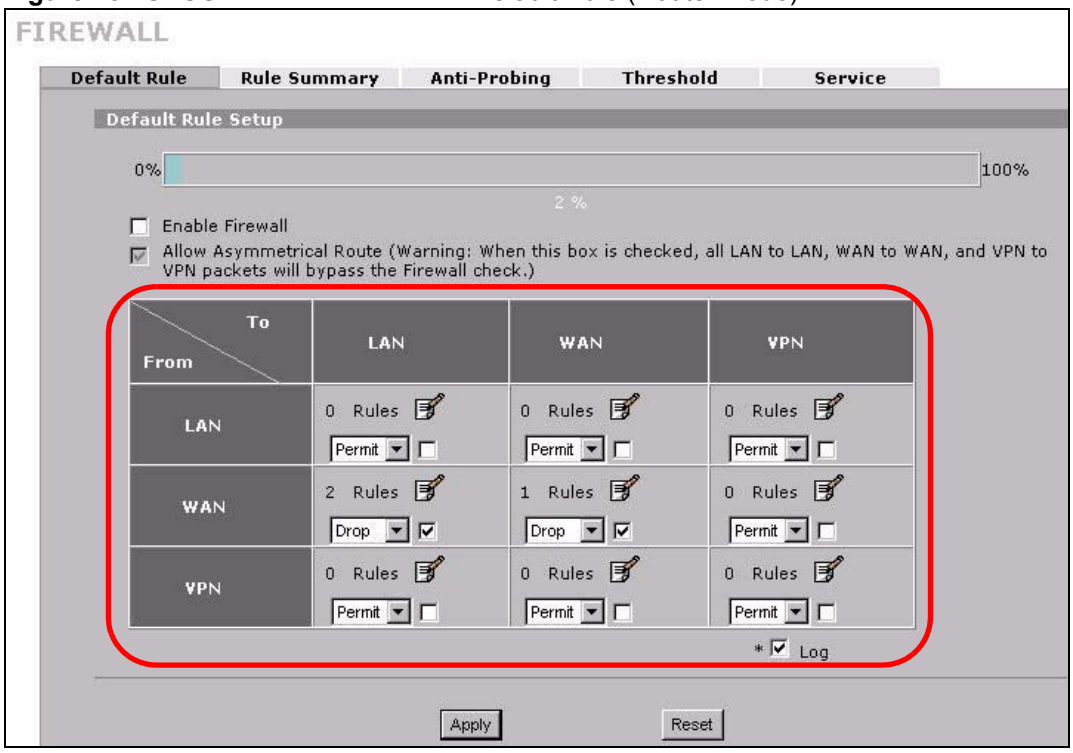
Your customized rules take precedence and override the ZyWALL's default settings. The ZyWALL checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyWALL takes the action specified in the rule.

9.2 Packet Direction Matrix

The ZyWALL's packet direction matrix allows you to apply certain security settings (like firewall, IDP and anti-virus) to traffic flowing in specific directions.

For example, click **SECURITY** > **FIREWALL** to open the following screen. This screen configures general firewall settings.

Figure 73 SECURITY > FIREWALL > Default Rule (Router Mode)

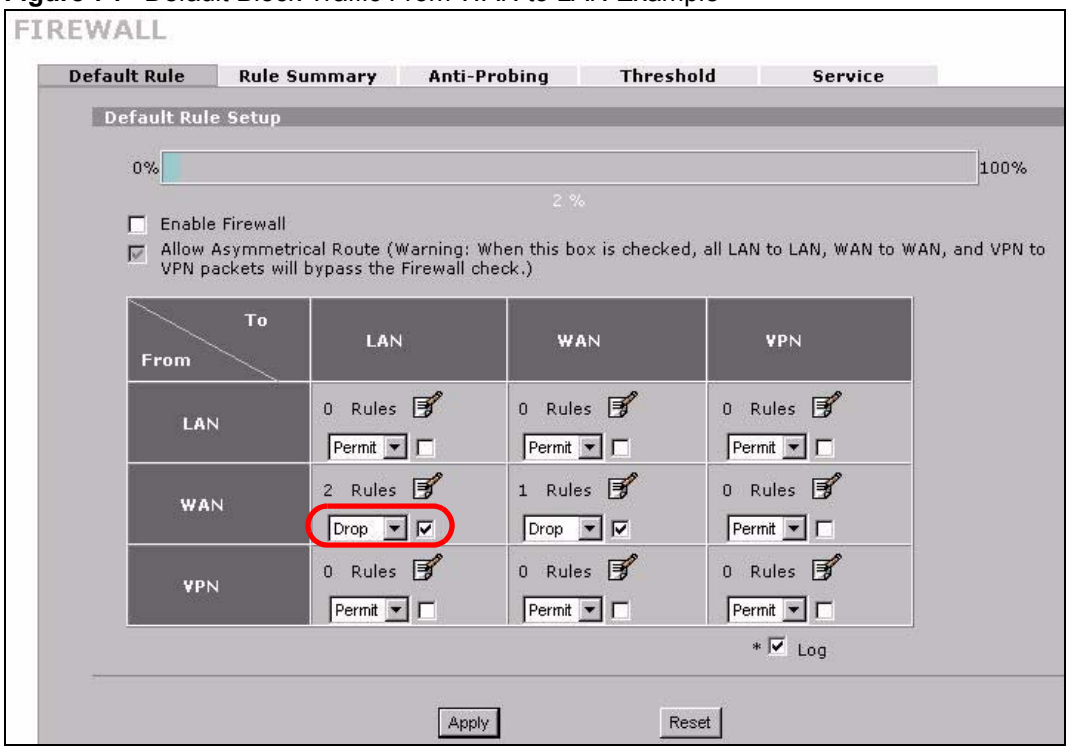


Packets have a source and a destination. The packet direction matrix in the lower part of the screen sets what the ZyWALL does with packets traveling in a specific direction that do not match any of the firewall rules.

From → To	
A specific interface or any of the ZyWALL's VPN connections	A specific interface or any of the ZyWALL's VPN connections

By default, the ZyWALL silently blocks traffic from WAN from going to the LAN interface. The field where the **From WAN** row and the **To LAN** column intersect is set to **Drop** as shown.

Figure 74 Default Block Traffic From WAN to LAN Example



9.3 Packet Direction Examples

Firewall rules are grouped based on the direction of travel of packets to which they apply. This section gives some examples of why you might configure firewall rules for specific connection directions.

By default, the ZyWALL allows packets traveling in the following directions.:

- LAN to LAN These rules specify which computers on the LAN can manage the ZyWALL (remote management) and communicate between networks or subnets connected to the LAN interface (IP alias).

  Note: You can also configure the remote management settings to allow only a specific computer to manage the ZyWALL.

- LAN to WAN These rules specify which computers on the LAN can access which computers or services connected to the WAN. See Section 9.5 on page 148 for an example.

By default, the ZyWALL drops packets traveling in the following directions.

- WAN to LAN — These rules specify which computers connected to the WAN can access which computers or services on the LAN. For example, you may create rules to:
  - Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
  - Allow public access to a Web server on your protected network. You could also block certain IP addresses from accessing it.

  Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN. See Section 16.5.3 on page 287 for an example.

- WAN to WAN — By default the ZyWALL stops computers connected to the WAN from managing the ZyWALL or using the ZyWALL as a gateway to communicate with other computers on the WAN. You could configure one of these rules to allow a WAN computer to manage the ZyWALL.

  Note: You must also configure the remote management settings to allow a WAN computer to manage the ZyWALL.

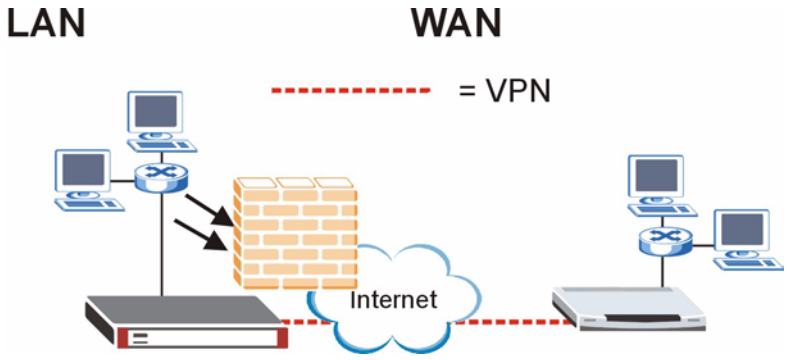
See Chapter 4 on page 81 for information about packets traveling to or from the VPN tunnels.

9.3.1 To VPN Packet Direction

The ZyWALL can apply firewall rules to traffic before encrypting it to send through the VPN tunnel. **To VPN** means traffic that comes in through the selected "from" interface and goes out through any of the ZyWALL's VPN tunnels. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through any of the ZyWALL's VPN tunnels.

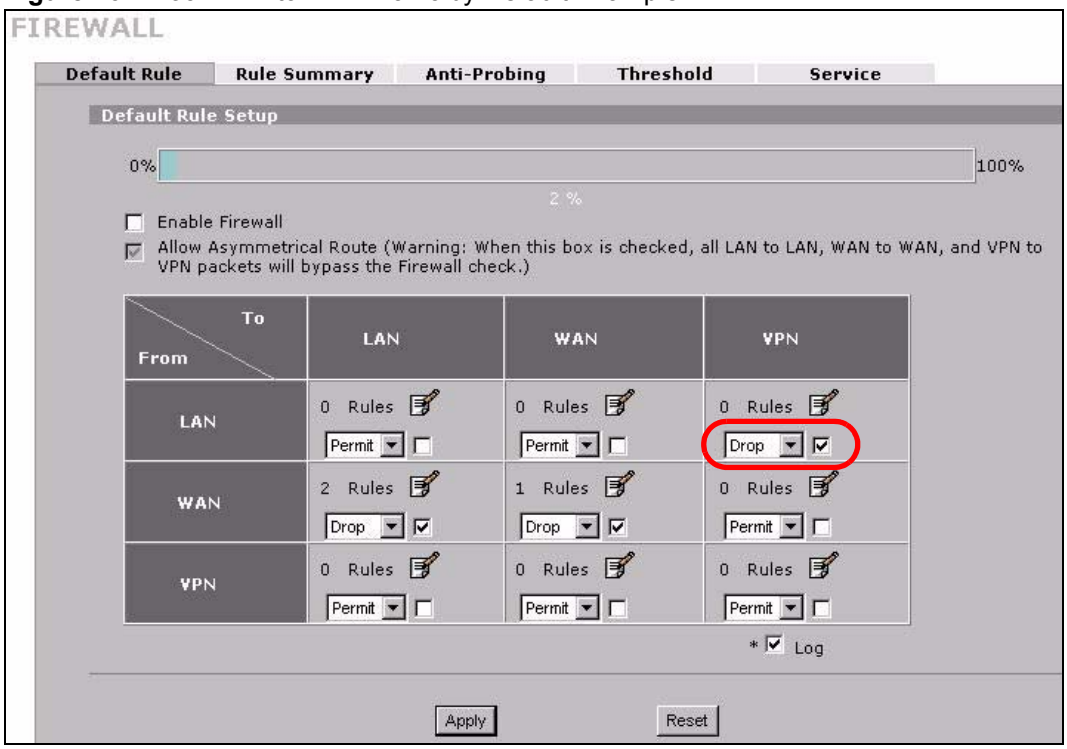
For example, you could configure the **From LAN To VPN** firewall rule to drop traffic from the LAN computers instead of sending it through the ZyWALL's VPN tunnel.

Figure 75 From LAN to VPN Example



In order to do this, you would configure the **SECURITY > FIREWALL > Default Rule** screen as follows.

Figure 76 Block LAN to VPN Traffic by Default Example

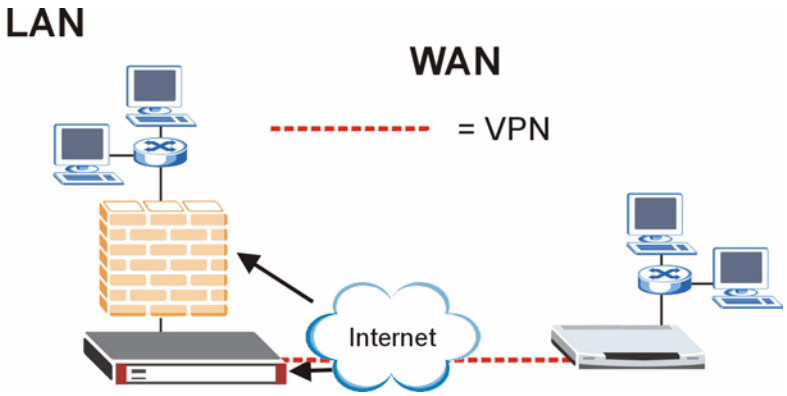


9.3.2 From VPN Packet Direction

You can also apply firewall rules to traffic that comes in through the ZyWALL's VPN tunnels. The ZyWALL decrypts the VPN traffic and then applies the firewall rules. **From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected "to" interface.

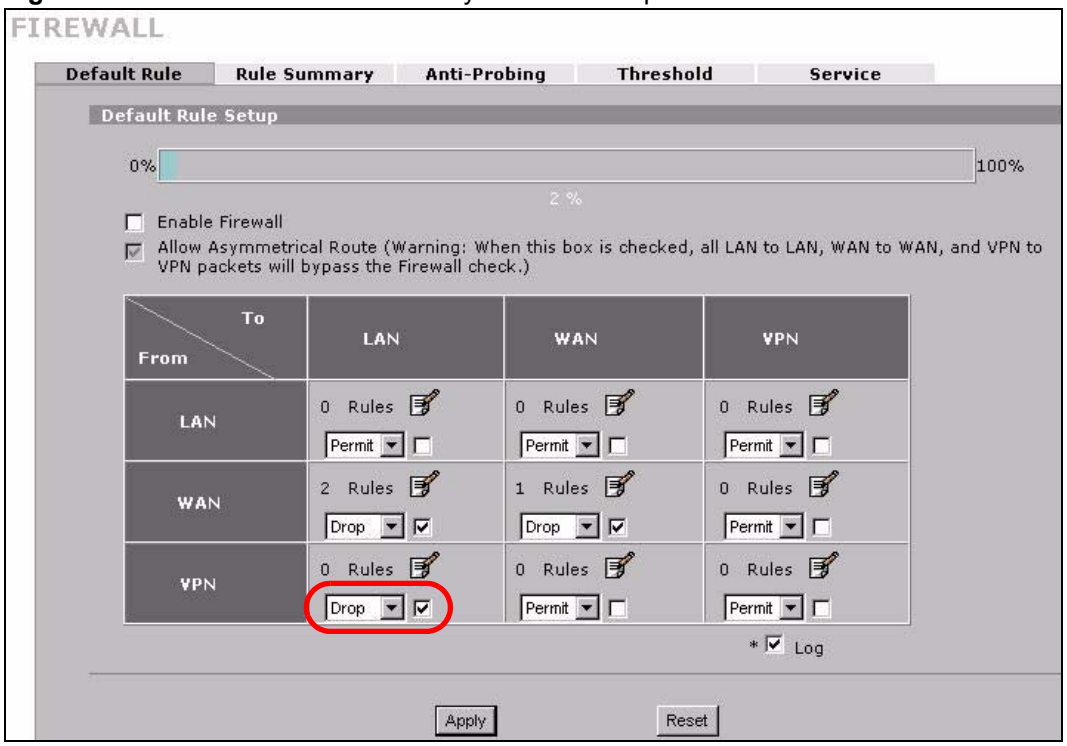
For example, by default the firewall allows traffic from the VPN tunnel to go to any of the ZyWALL's interfaces, the ZyWALL itself and other VPN tunnels. You could edit the **From VPN To LAN** default firewall rule to silently block traffic from the VPN tunnels from going to the LAN computers.

Figure 77 From VPN to LAN Example



In order to do this, you would configure the **SECURITY > FIREWALL > Default Rule** screen as follows.

Figure 78 Block VPN to LAN Traffic by Default Example

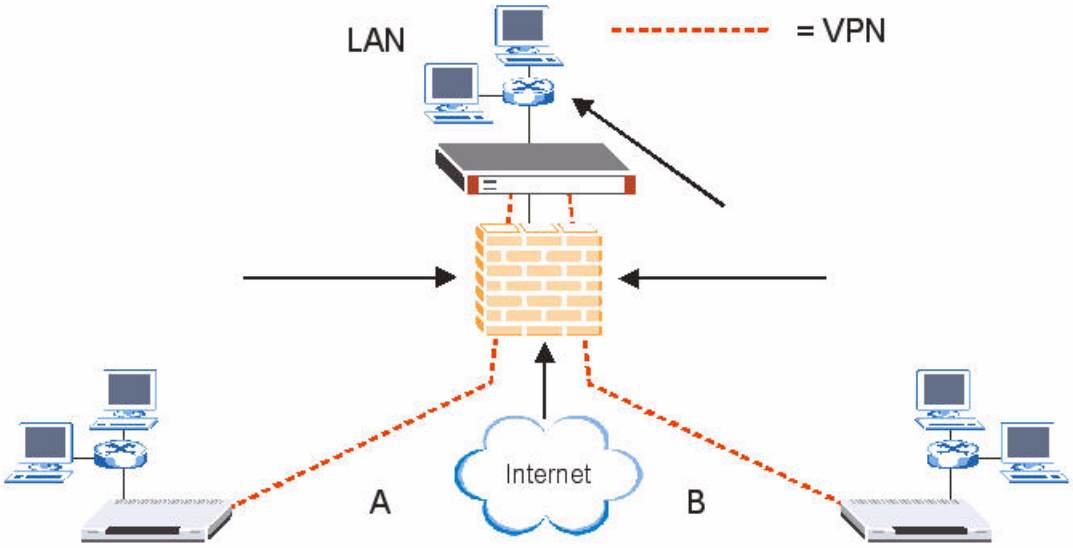


9.3.3 From VPN To VPN Packet Direction

From VPN To VPN firewall rules apply to traffic that comes in through the ZyWALL's VPN tunnel and terminates at the ZyWALL (like for remote management). The ZyWALL decrypts the traffic and applies the firewall rules before allowing the traffic to terminate at the ZyWALL.

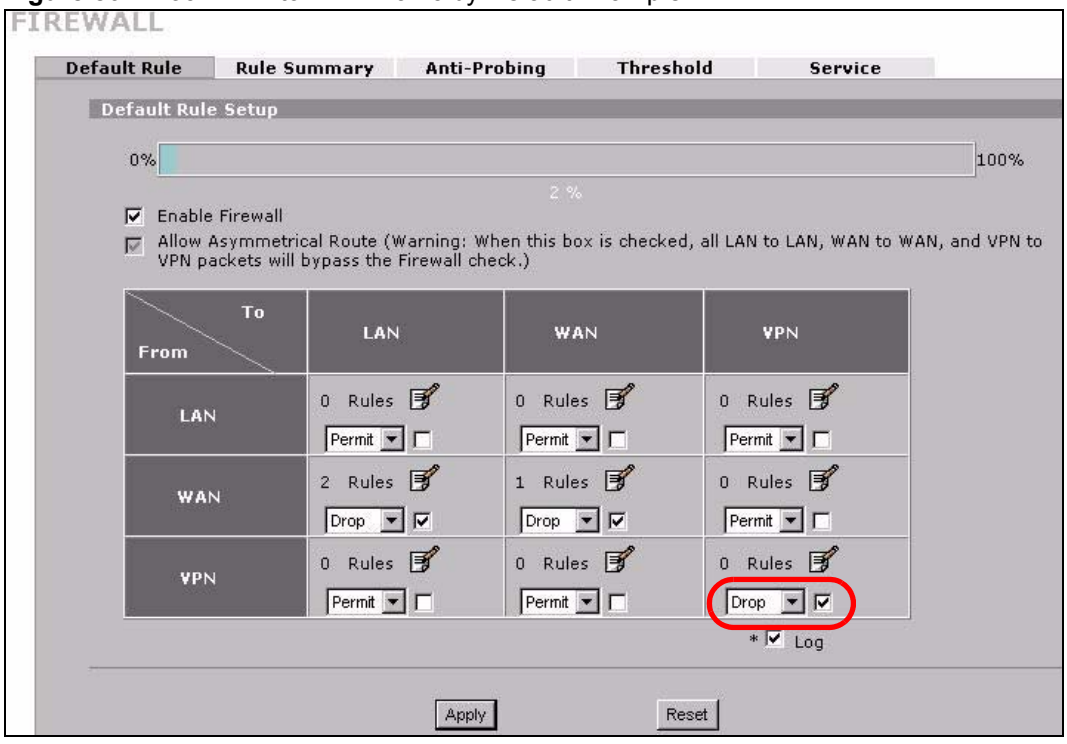
In the following example, the **From VPN To VPN** default firewall rule silently blocks the traffic that the ZyWALL receives from any VPN tunnel (either A or B) that is destined for the other VPN tunnel or the ZyWALL itself. VPN traffic destined for the DMZ is allowed through.

Figure 79 From VPN to VPN Example



You would configure the **SECURITY > FIREWALL > Default Rule** screen as follows.

Figure 80 Block VPN to VPN Traffic by Default Example



9.4 Security Considerations

Incorrectly configuring the firewall may block valid access or introduce security risks to the ZyWALL and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

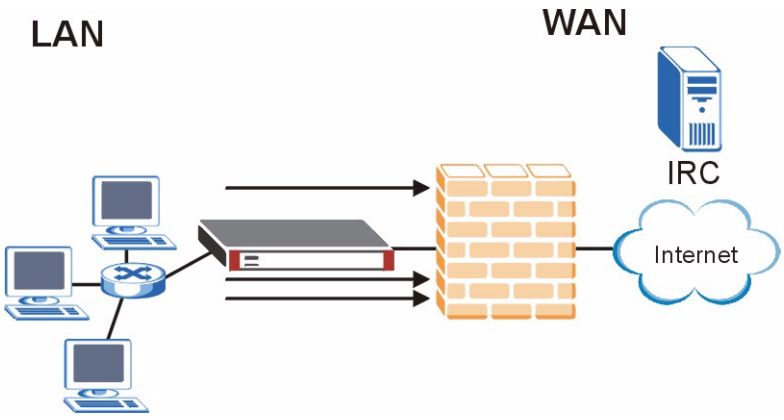
1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.

9.5 Firewall Rules Example

Suppose that your company decides to block all of the LAN users from using IRC (Internet Relay Chat) through the Internet. To do this, you would configure a LAN to WAN firewall rule that blocks IRC traffic from any source IP address from going to any destination address. You do not need to specify a schedule since you need the firewall rule to always be in effect. The following figure shows the results of this rule.

Figure 81 Blocking All LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

Table 37 Blocking All LAN to WAN IRC Traffic Example

#	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	Any	Any	Any	IRC	Drop
Default	Any	Any	Any	Any	Allow

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the firewall's default policy that allows all traffic from the LAN to go to the WAN.

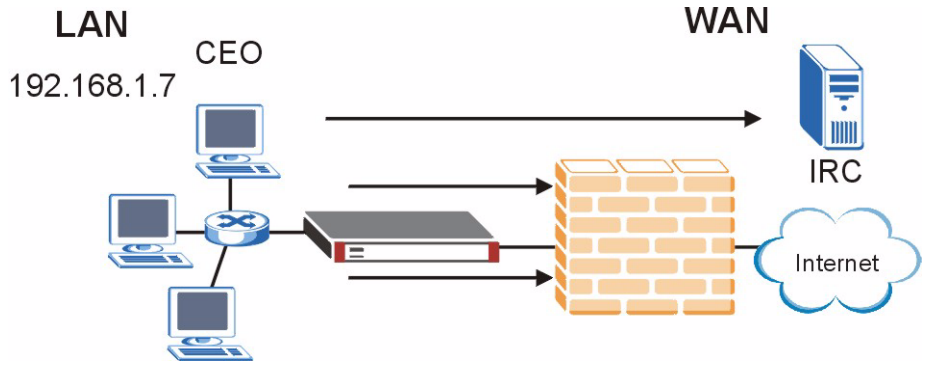
The ZyWALL applies the firewall rules in order. So for this example, when the ZyWALL receives traffic from the LAN, it checks it against the first rule. If the traffic matches (if it is IRC traffic) the firewall takes the action in the rule (drop) and stops checking the firewall rules. Any traffic that does not match the first firewall rule will match the default rule and the ZyWALL forwards it.

Now suppose that your company wants to let the CEO use IRC. You can configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer. In order to make sure that the CEO's computer always uses the same IP address, make sure it either:

- has a static IP address,
- or you configure a static DHCP entry for it so the ZyWALL always assigns it the same IP address (see Section 6.9 on page 113 for information on static DHCP).

Now you configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer (192.168.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the firewall rule to always be in effect. The following figure shows the results of your two custom rules.

Figure 82 Limited LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

Table 38 Limited LAN to WAN IRC Traffic Example

#	SOURCE	DESTINATION	SCHEDULE	SERVICE	ACTION
1	192.168.1.7	Any	Any	IRC	Allow
2	Any	Any	Any	IRC	Drop
Default	Any	Any	Any	Any	Allow

- The first row allows the LAN computer at IP address 192.168.1.7 to access the IRC service on the WAN.
- The second row blocks LAN access to the IRC service on the WAN.
- The third row is (still) the firewall's default policy of allowing all traffic from the LAN to go to the WAN.

The rule for the CEO must come before the rule that blocks all LAN to WAN IRC traffic. If the rule that blocks all LAN to WAN IRC traffic came first, the CEO's IRC traffic would match that rule and the ZyWALL would drop it and not check any other firewall rules.

9.6 Asymmetrical Routes

If an alternate gateway on the LAN has an IP address in the same subnet as the ZyWALL's LAN IP address, return traffic may not go through the ZyWALL. This is called an asymmetrical or "triangle" route. This causes the ZyWALL to reset the connection, as the connection has not been acknowledged.

You can have the ZyWALL permit the use of asymmetrical route topology on the network (not reset the connection).

Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyWALL. A better solution is to use IP alias to put the ZyWALL and the backup gateway on separate subnets.

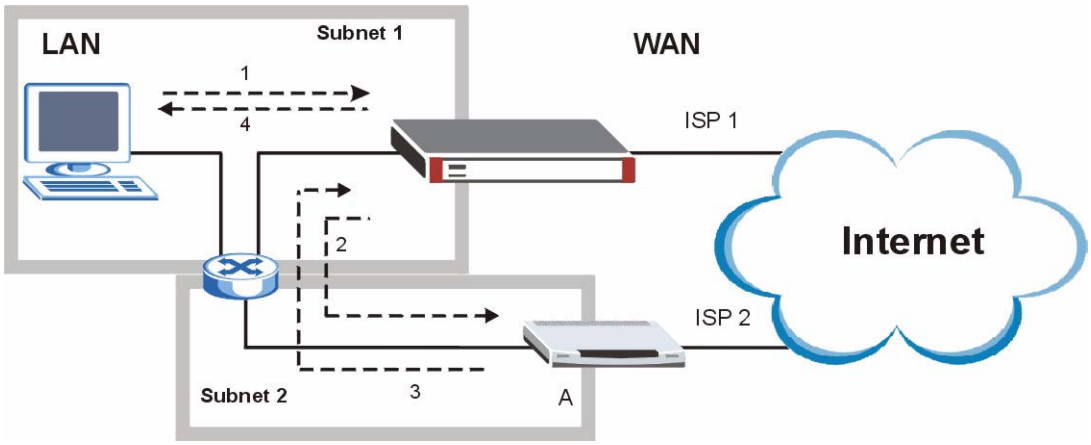
9.6.1 Asymmetrical Routes and IP Alias

You can use IP alias instead of allowing asymmetrical routes. IP Alias allow you to partition your network into logical sections over the same interface.

By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the ZyWALL to your LAN. The following steps describe such a scenario.

1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The ZyWALL reroutes the packet to Gateway **A**, which is in **Subnet 2**.
3. The reply from the WAN goes to the ZyWALL.
4. The ZyWALL then sends it to the computer on the LAN in **Subnet 1**.

Figure 83 Using IP Alias to Solve the Triangle Route Problem

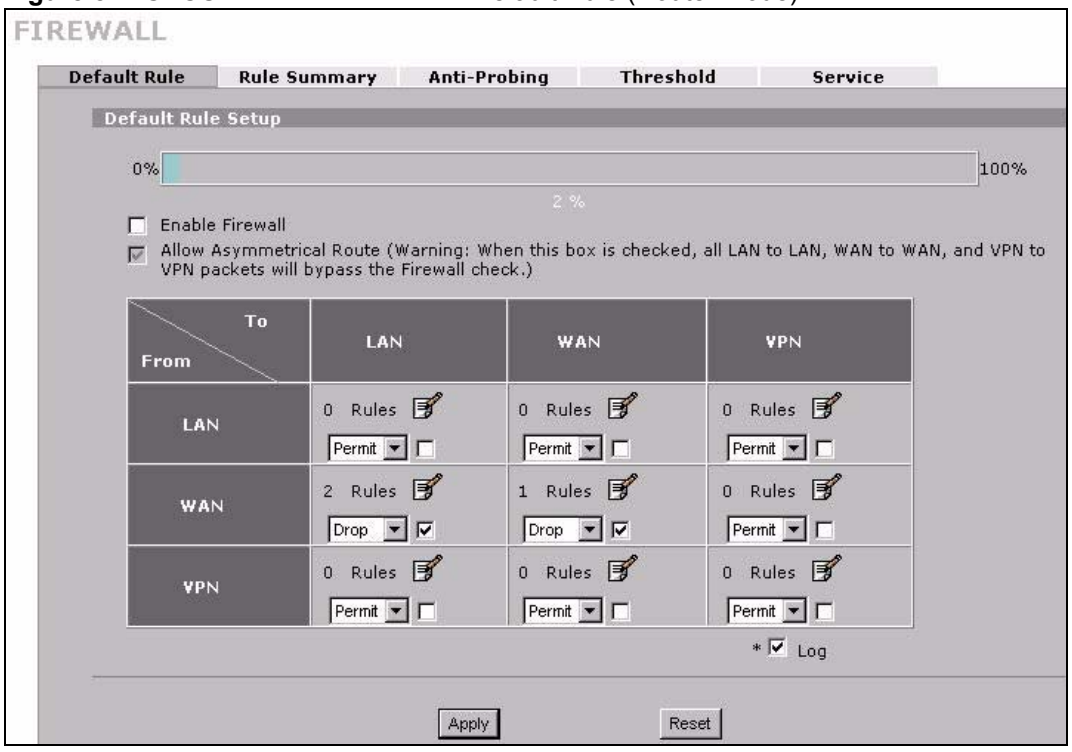


9.7 Firewall Default Rule (Router Mode)

Click **SECURITY** > **FIREWALL** to open the **Default Rule** screen.

Use this screen to configure general firewall settings when the ZyWALL is set to router mode.

Figure 84 SECURITY > FIREWALL > Default Rule (Router Mode)



The following table describes the labels in this screen.

Table 39 SECURITY > FIREWALL > Default Rule (Router Mode)

LABEL	DESCRIPTION
0-100%	This bar displays the percentage of the ZyWALL's firewall rules storage space that is currently in use. When the storage space is almost full, you should consider deleting unnecessary firewall rules before adding more firewall rules.
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated. Note: When you activate the firewall, all current connections through the ZyWALL are dropped when you apply your changes.
Allow Asymmetrical Route	If an alternate gateway on the LAN has an IP address in the same subnet as the ZyWALL's LAN IP address, return traffic may not go through the ZyWALL. This is called an asymmetrical or "triangle" route. This causes the ZyWALL to reset the connection, as the connection has not been acknowledged. Select this check box to have the ZyWALL permit the use of asymmetrical route topology on the network (not reset the connection). Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyWALL. A better solution is to use IP alias to put the ZyWALL and the backup gateway on separate subnets. See Section 9.6.1 on page 150 for an example.

Table 39 SECURITY > FIREWALL > Default Rule (Router Mode) (continued)

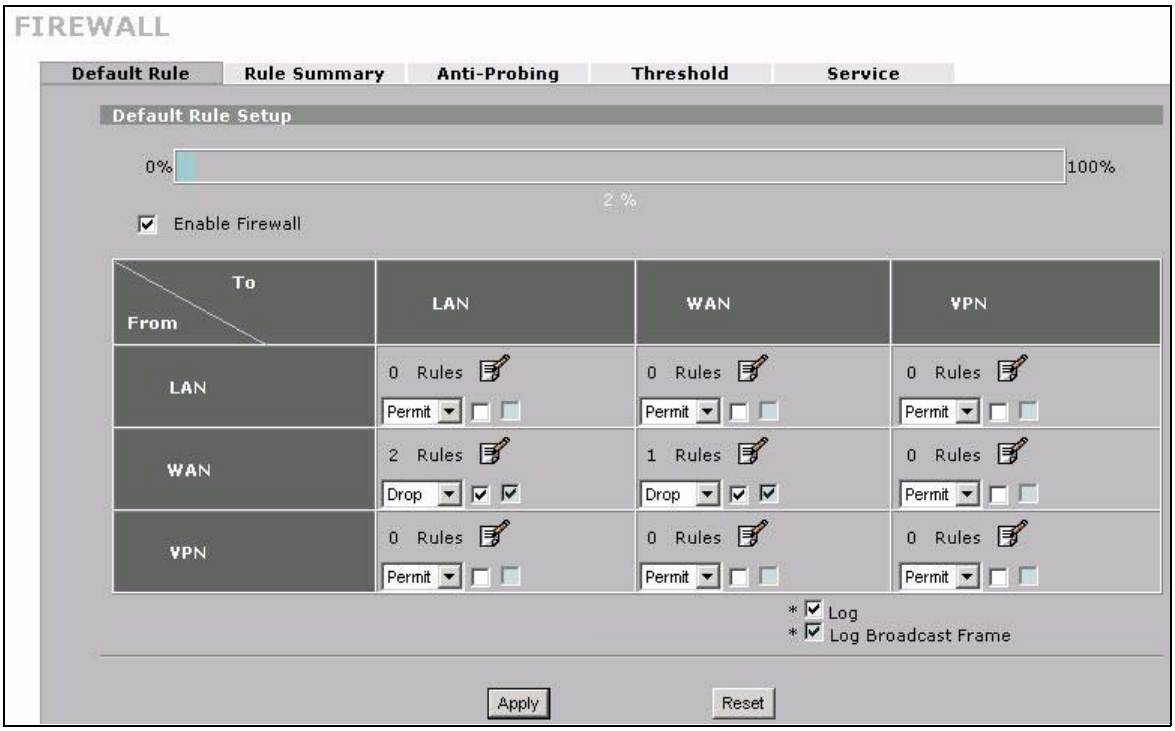
LABEL	DESCRIPTION
From, To	The firewall rules are grouped by the direction of packet travel. The number of rules for each packet direction displays. Click **Edit** to go to a summary screen of the rules for that packet direction. Here are some example descriptions of the directions of travel. **From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the ZyWALL or the ZyWALL itself. The ZyWALL does not apply the firewall to packets traveling from a LAN computer to another LAN computer on the same subnet. **From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected “to” interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN. The ZyWALL applies the firewall to the traffic after decrypting it. **To VPN** is traffic that comes in through the selected “from” interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The ZyWALL applies the firewall to the traffic before encrypting it. **From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel or terminates at the ZyWALL. This is the case when the ZyWALL is the hub in a hub-and-spoke VPN. This is also the case if you allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the ZyWALL. The ZyWALL applies the firewall to the traffic after decrypting it. Note: The VPN connection directions apply to the traffic going to or from the ZyWALL’s VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic). Use the drop-down list box to set the firewall’s default actions based on the direction of travel of packets. Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select **Permit** to allow the passage of the packets. The firewall rules is for the WAN port with a higher route priority.
Log	Select the check box next to a direction of packet travel to create a log when the above action is taken for packets that are traveling in that direction and do not match any of your customized rules.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

9.8 Firewall Default Rule (Bridge Mode)

Click **SECURITY** > **FIREWALL** to open the **Default Rule** screen.

Use this screen to configure general firewall settings when the ZyWALL is set to bridge mode. See Section 9.1 on page 141 for more information about the firewall.

Figure 85 SECURITY > FIREWALL > Default Rule (Bridge Mode)



The following table describes the labels in this screen.

Table 40 SECURITY > FIREWALL > Default Rule (Bridge Mode)

LABEL	DESCRIPTION
0-100%	This bar displays the percentage of the ZyWALL's firewall rules storage space that is currently in use. When the storage space is almost full, you should consider deleting unnecessary firewall rules before adding more firewall rules.
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated. Note: When you activate the firewall, all current connections through the ZyWALL are dropped when you apply your changes.

Table 40 SECURITY > FIREWALL > Default Rule (Bridge Mode)

LABEL	DESCRIPTION
From, To	The firewall rules are grouped by the direction of packet travel. The number of rules for each packet direction. Click **Edit** to go to a summary screen of the rules for that packet direction. Here are some example descriptions of the directions of travel. **From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the ZyWALL or the ZyWALL itself. The ZyWALL does not apply the firewall to packets traveling from a LAN computer to another LAN computer on the same subnet. **From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN. The ZyWALL applies the firewall to the traffic after decrypting it. **To VPN** is traffic that comes in through the selected "from" interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The ZyWALL applies the firewall to the traffic before encrypting it. **From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel or terminates at the ZyWALL. This is the case when the ZyWALL is the hub in a hub-and-spoke VPN. This is also the case if you allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the ZyWALL. The ZyWALL applies the firewall to the traffic after decrypting it. Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic). Use the drop-down list box to set the firewall's default actions based on the direction of travel of packets. Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select **Permit** to allow the passage of the packets. The firewall rules is for the WAN port with a higher route priority.
Log	Select this to create a log when the above action is taken.
Log Broadcast Frame	Select this to create a log for any broadcast frames traveling in the selected direction. Many of these logs in a short time period could indicate a broadcast storm. A broadcast storm occurs when a packet triggers multiple responses from all hosts on a network or when computers attempt to respond to a host that never replies. As a result, duplicated packets are continuously created and circulated in the network, thus reducing network performance or even rendering it inoperable. A broadcast storm can be caused by an attack on the network, an incorrect network topology (such as a bridge loop) or a malfunctioning network device.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

9.9 Firewall Rule Summary

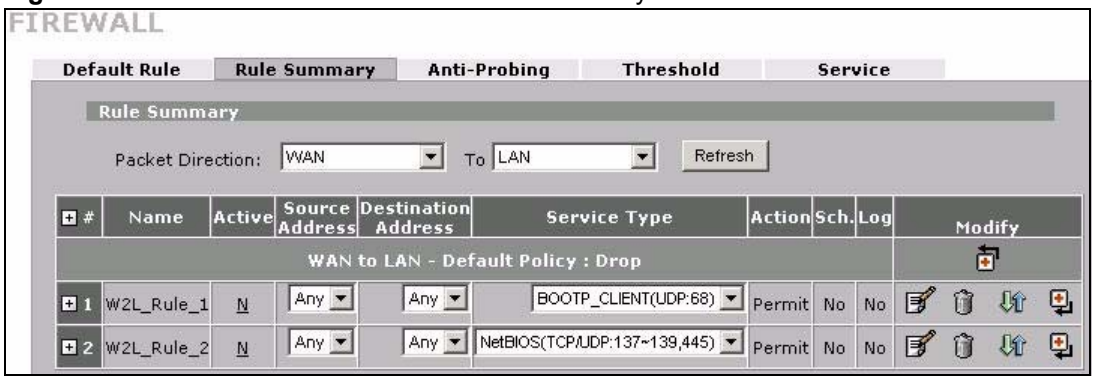
Click **SECURITY** > **FIREWALL** > **Rule Summary** to open the screen. This screen displays a list of the configured firewall rules.

The ordering of your rules is very important as rules are applied in the order that they are listed.

See Section 9.1 on page 141 for more information about the firewall.

- When the ZyWALL is in bridge mode, enable the default **WAN to LAN** firewall rule for the **BOOTP_CLIENT** service to let DHCP clients behind the ZyWALL use a DHCP server on the WAN.
- Enable the default **WAN to LAN** firewall rule for the **NetBIOS** service to let computers behind the ZyWALL access devices on the WAN using computer names.

Figure 86 SECURITY > FIREWALL > Rule Summary



The following table describes the labels in this screen.

Table 41 SECURITY > FIREWALL > Rule Summary

LABEL	DESCRIPTION
Packet Direction	Use the drop-down list boxes and click **Refresh** to select a direction of travel of packets for which you want to display firewall rules. Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic).
+/-	In the heading row, click + to expand or - to collapse the **Source Address**, **Destination Address** and **Service Type** drop down lists for all of the displayed rules.
Default Policy	This field displays the default action you selected in the **Default Rule** screen for the packet direction displayed.
The following fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above.	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. Click + to expand or - to collapse the **Source Address**, **Destination Address** and **Service Type** drop down lists.
Name	This is the name of the firewall rule.
Active	This field displays whether a firewall is turned on (**Y**) or not (**N**). Click the letter to change it to the other state (click **Y** to change it to **N** or **N** to change it to **Y**).

Table 41 SECURITY > FIREWALL > Rule Summary

LABEL	DESCRIPTION
Source Address	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Destination Address	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Service Type	This drop-down list box displays the services to which this firewall rule applies. Custom services have an * before the name. See Appendix D on page 463 for a list of common services.
Action	This field displays whether the firewall silently discards packets (**Drop**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**Reject**) or allows the passage of packets (**Permit**).
Sch.	This field tells you whether a schedule is specified (**Yes**) or not (**No**).
Log	This field shows you whether a log is created when packets match this rule (**Yes**) or not (**No**).
Modify	Click the edit icon to go to the screen where you can edit the rule. Click the delete icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action. Click the move icon, type an index number, and press Enter to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering. Click the insert icon to display the screen where you can configure a new firewall rule. The insert icon at the top of the row creates the new firewall rule before the others. The individual firewall rule insert icons create a new firewall rule after the row's firewall rule.

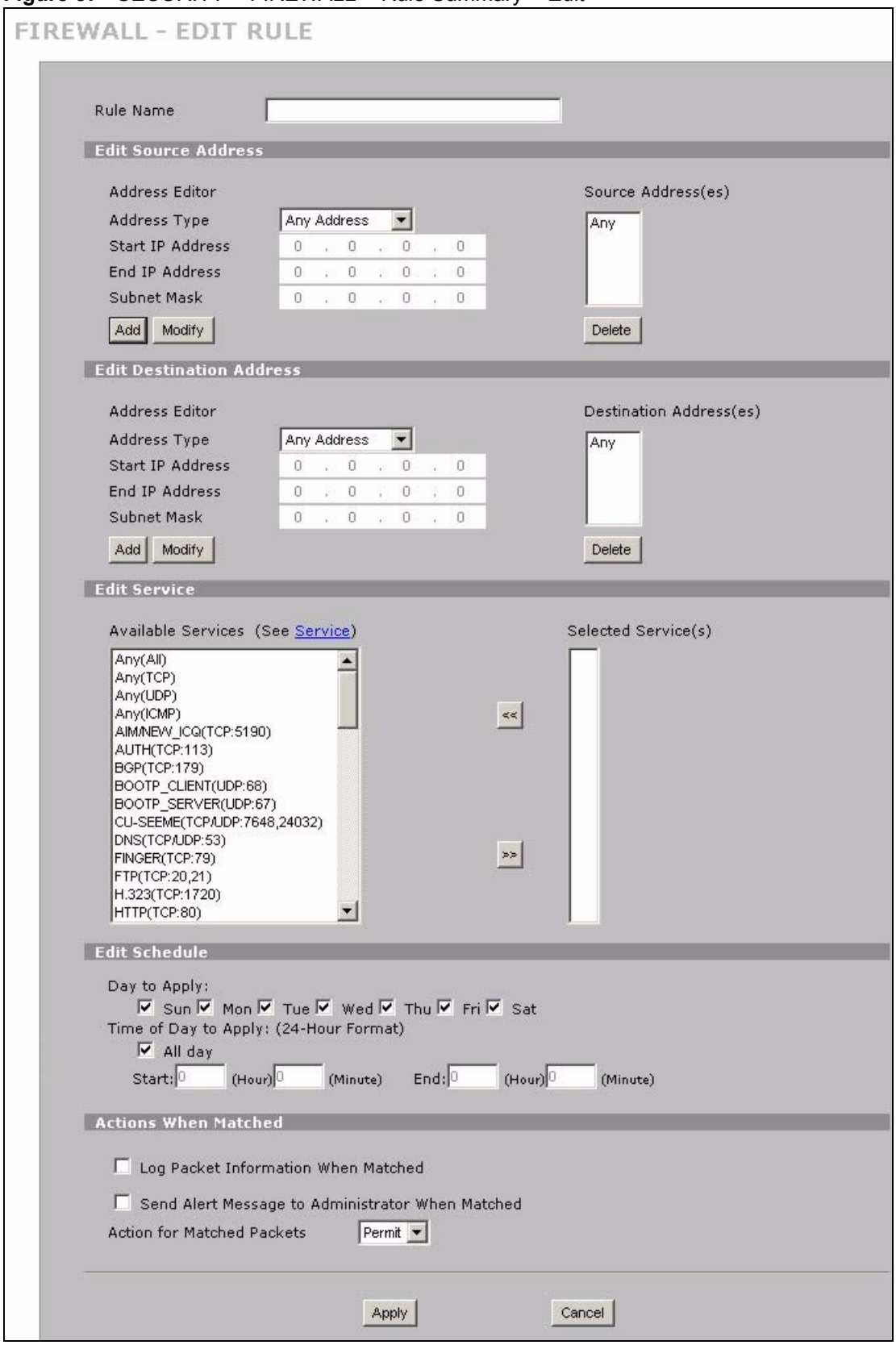
9.9.1 Firewall Edit Rule

In the **Rule Summary** screen, click the edit icon or the insert icon to display the **Firewall Edit Rule** screen.

Use this screen to create or edit a firewall rule. Refer to the following table for information on the labels.

See Section 9.1 on page 141 for more information about the firewall.

Figure 87 SECURITY > FIREWALL > Rule Summary > Edit



The following table describes the labels in this screen.

Table 42 SECURITY > FIREWALL > Rule Summary > Edit

LABEL	DESCRIPTION
Rule Name	Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the firewall rule. Spaces are allowed.
Edit Source/ Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add	Click **Add** to add a new address to the **Source** or **Destination Address(es)** box. You can add multiple addresses, ranges of addresses, and/or subnets.
Modify	To edit an existing source or destination address, select it from the box and click **Modify**.
Delete	Highlight an existing source or destination address from the **Source** or **Destination Address(es)** box above and click **Delete** to remove it.
Edit Service	
Available/ Selected Services	Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Service(s)** box on the right. To remove a service, highlight it in the **Selected Service(s)** box on the right, then click **<<**. Custom services have an * before the name. Next to the name of a service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type). For example, look at the DNS entry, (UDP/TCP:53) means UDP port 53 and TCP port 53. Click the **Service** link to go to the **Service screen where you can** configure custom service ports. See Appendix D on page 463 for a list of commonly used services and port numbers. You can use the [CTRL] key and select multiple services at once.
Edit Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select **All Day** or enter the start and end times in the hour-minute format to apply the rule.
Actions When Matched	
Log Packet Information When Matched	This field determines if a log for packets that match the rule is created (**Yes**) or not (**No**). Go to the **Log Settings** page and select the **Access Control** logs category to have the ZyWALL record these logs.
Send Alert Message to Administrator When Matched	Select the check box to have the ZyWALL generate an alert when the rule is matched.

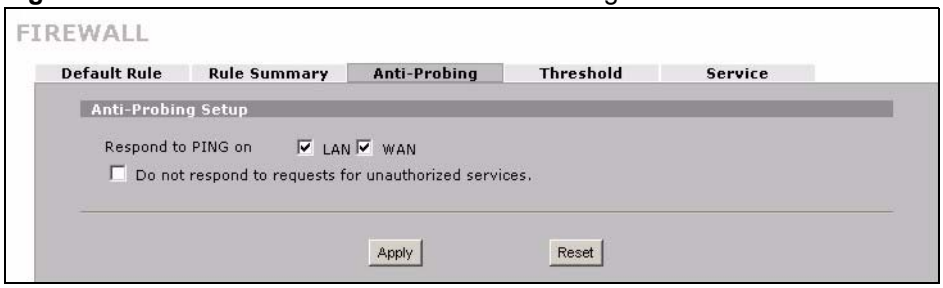
Table 42 SECURITY > FIREWALL > Rule Summary > Edit

LABEL	DESCRIPTION
Action for Matched Packets	Use the drop-down list box to select what the firewall is to do with packets that match this rule. Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender. Select **Permit** to allow the passage of the packets. Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) if you want to allow computers on the WAN to access devices on the LAN. Note: You may also need to configure the remote management settings if you want to allow a WAN computer to manage the ZyWALL or restrict management from the LAN.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

9.10 Anti-Probing

Click **SECURITY > FIREWALL > Anti-Probing** to open the following screen. Configure this screen to help keep the ZyWALL hidden from probing attempts. You can specify which of the ZyWALL's interfaces will respond to Ping requests and whether or not the ZyWALL is to respond to probing for unused ports.

Figure 88 SECURITY > FIREWALL > Anti-Probing



The following table describes the labels in this screen.

Table 43 SECURITY > FIREWALL > Anti-Probing

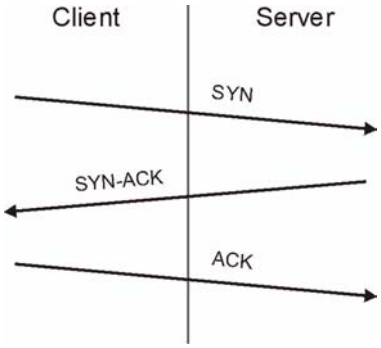
LABEL	DESCRIPTION
Respond to PING on	Select the check boxes of the interfaces that you want to reply to incoming Ping requests. Clear an interface's check box to have the ZyWALL not respond to any Ping requests that come into that interface.
Do not respond to requests for unauthorized services.	Select this option to prevent hackers from finding the ZyWALL by probing for unused ports. If you select this option, the ZyWALL will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyWALL unseen. If this option is not selected, the ZyWALL will reply with an ICMP port unreachable packet for a port probe on its unused UDP ports and a TCP reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the ZyWALL's firewall rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the ZyWALL reacts based on the firewall rule to either send a TCP reset packet for a blocked TCP packet (or an ICMP port-unreachable packet for a blocked UDP packets) or just drop the packets without sending a response packet.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

9.11 Firewall Thresholds

For DoS attacks, the ZyWALL uses thresholds to determine when to start dropping sessions that do not become fully established (half-open sessions). These thresholds apply globally to all sessions.

For TCP, half-open means that the session has not reached the established state-the TCP three-way handshake has not yet been completed. Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

Figure 89 Three-Way Handshake



For UDP, half-open means that the firewall has detected no return traffic. An unusually high number (or arrival rate) of half-open sessions could indicate a DOS attack.

9.11.1 Threshold Values

If everything is working properly, you probably do not need to change the threshold settings as the default threshold values should work for most small offices. Tune these parameters when you believe the ZyWALL has been receiving DoS attacks that are not recorded in the logs or the logs show that the ZyWALL is classifying normal traffic as DoS attacks. Factors influencing choices for threshold values are:

1. The maximum number of opened sessions.
2. The minimum capacity of server backlog in your LAN network.
3. The CPU power of servers in your LAN network.
4. Network bandwidth.
5. Type of traffic for certain servers.

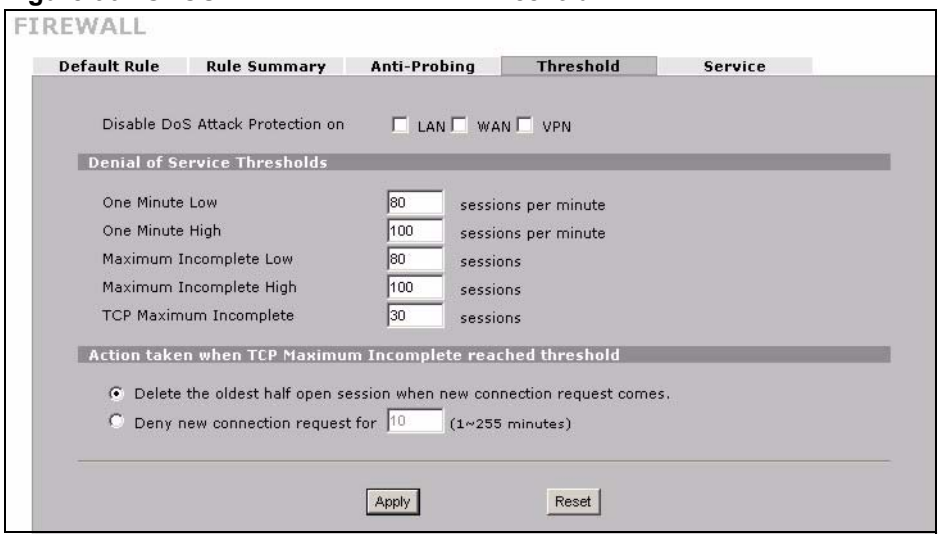
Reduce the threshold values if your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy).

If you often use P2P applications such as file sharing with eMule or eDonkey, it's recommended that you increase the threshold values since lots of sessions will be established during a small period of time and the ZyWALL may classify them as DoS attacks.

9.12 Threshold Screen

Click **SECURITY > FIREWALL > Threshold** to bring up the next screen. The global values specified for the threshold and timeout apply to all TCP connections.

Figure 90 SECURITY > FIREWALL > Threshold



The following table describes the labels in this screen.

Table 44 SECURITY > FIREWALL > Threshold

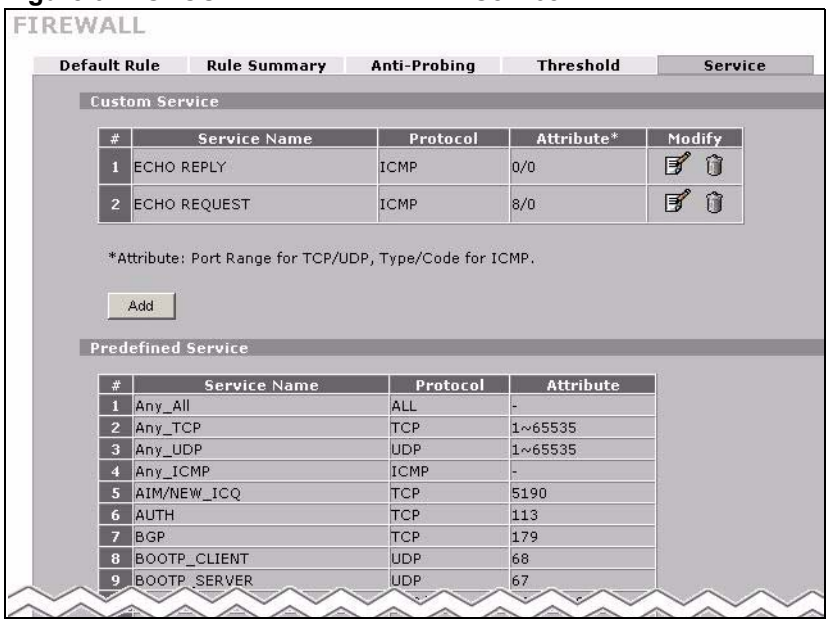
LABEL	DESCRIPTION
Disable DoS Attack Protection on	Select the check boxes of any interfaces (or all VPN tunnels) for which you want the ZyWALL to not use the Denial of Service protection thresholds. This disables DoS protection on the selected interface (or all VPN tunnels). You may want to disable DoS protection for an interface if the ZyWALL is treating valid traffic as DoS attacks. Another option would be to raise the thresholds.
Denial of Service Thresholds	The ZyWALL measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.
One Minute Low	This is the rate of new half-open sessions per minute that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.
One Minute High	This is the rate of new half-open sessions per minute that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection attempts. For example, if you set the one minute high to 100, the ZyWALL starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number. For example, if you set the maximum incomplete high to 100, the ZyWALL starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low.
TCP Maximum Incomplete	An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host. Specify the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth. The ZyWALL sends alerts whenever the **TCP Maximum Incomplete** is exceeded.
Action taken when TCP Maximum Incomplete reached threshold	Select the action that ZyWALL should take when the TCP maximum incomplete threshold is reached. You can have the ZyWALL either: Delete the oldest half open session when a new connection request comes. or Deny new connection requests for the number of minutes that you specify (between 1 and 256).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

9.13 Service

Click **SECURITY > FIREWALL** > **Service** to open the screen as shown next. Use this screen to configure custom services for use in firewall rules or view the services that are predefined in the ZyWALL.

See Section 9.1 on page 141 for more information about the firewall.

Figure 91 SECURITY > FIREWALL > Service



The following table describes the labels in this screen.

Table 45 SECURITY > FIREWALL > Service

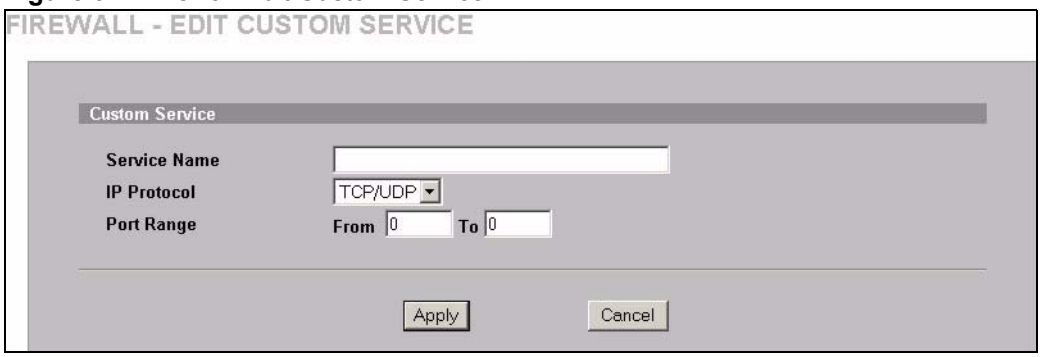
LABEL	DESCRIPTION
Custom Service	This table shows all configured custom services.
#	This is the index number of the custom service.
Service Name	This is the name of the service.
Protocol	This is the IP protocol type. If you selected **Custom**, this is the IP protocol value you entered.
Attribute	This is the IP port number or ICMP type and code that defines the service.
Modify	Click the edit icon to go to the screen where you can edit the service. Click the delete icon to remove an existing service. A window displays asking you to confirm that you want to delete the service. Note that subsequent services move up by one when you take this action.
Add	Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Predefined Service	This table shows all the services that are already configured for use in firewall rules. See Appendix D on page 463 for a list of common services.
#	This is the index number of the predefined service.
Service Name	This is the name of the service.
Protocol	This is the IP protocol type. There may be more than one IP protocol type.
Attribute	This is the IP port number or ICMP type and code that defines the service.

9.13.1 Firewall Edit Custom Service

Click **SECURITY > FIREWALL** > **Service** > **Add** to display the following screen. Use this screen to configure a custom service entry not is not predefined in the ZyWALL. See Appendix D on page 463 the user's guide appendices for a list of commonly used services and port numbers.

See Section 9.1 on page 141 for more information about the firewall.

Figure 92 Firewall Edit Custom Service



The following table describes the labels in this screen.

Table 46 SECURITY > FIREWALL > Service > Add

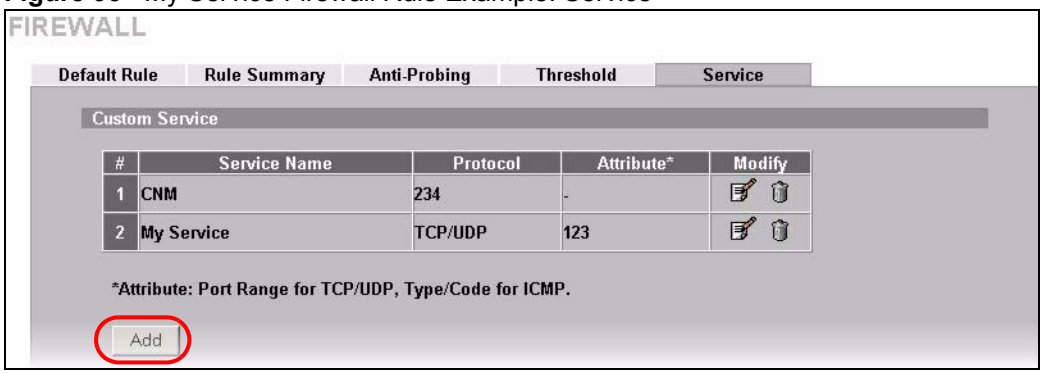
LABEL	DESCRIPTION
Service Name	Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the custom service. You cannot use the "(" character. Spaces are allowed.
IP Protocol	Choose the IP protocol (**TCP**, **UDP**, **TCP/UDP**, **ICMP** or **Custom**) that defines your customized service from the drop down list box. If you select **Custom**, specify the protocol's number. For example, ICMP is 1, TCP is 6, UDP is 17 and so on.
Port Range	Enter the port number (from 1 to 255) that defines the customized service To specify one port only, enter the port number in the **From** field and enter it again in the **To** field. To specify a span of ports, enter the first port in the **From** field and enter the last port in the **To** field.
Type/Code	This field is available only when you select **ICMP** in the **IP Protocol** field. The ICMP messages are identified by their types and in some cases codes. Enter the type number in the **Type** field and select the **Code** radio button and enter the code number if any.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

9.14 My Service Firewall Rule Example

The following Internet firewall rule example allows a hypothetical My Service connection from the Internet.

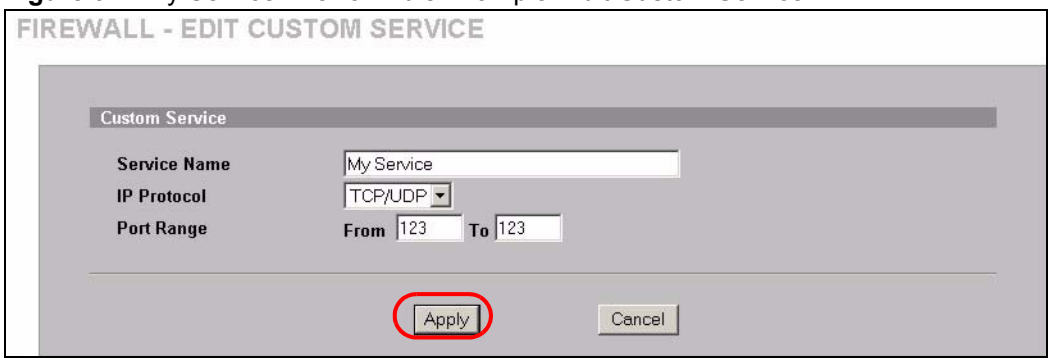
1 In the **Service** screen, click **Add** to open the **Edit Custom Service** screen.

Figure 93 My Service Firewall Rule Example: Service



2 Configure it as follows and click **Apply**.

Figure 94 My Service Firewall Rule Example: Edit Custom Service

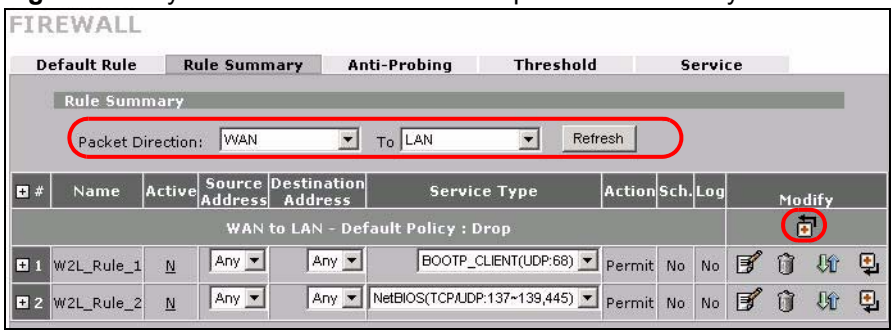


3 Click **Rule Summary**. Select **WAN to LAN** from the **Packet Direction** drop-down list box.

4 In the **Rule Summary** screen, type the index number for where you want to put the rule. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

5 Click **Insert** at the top of the **Modify** column to display the firewall rule configuration screen.

Figure 95 My Service Firewall Rule Example: Rule Summary

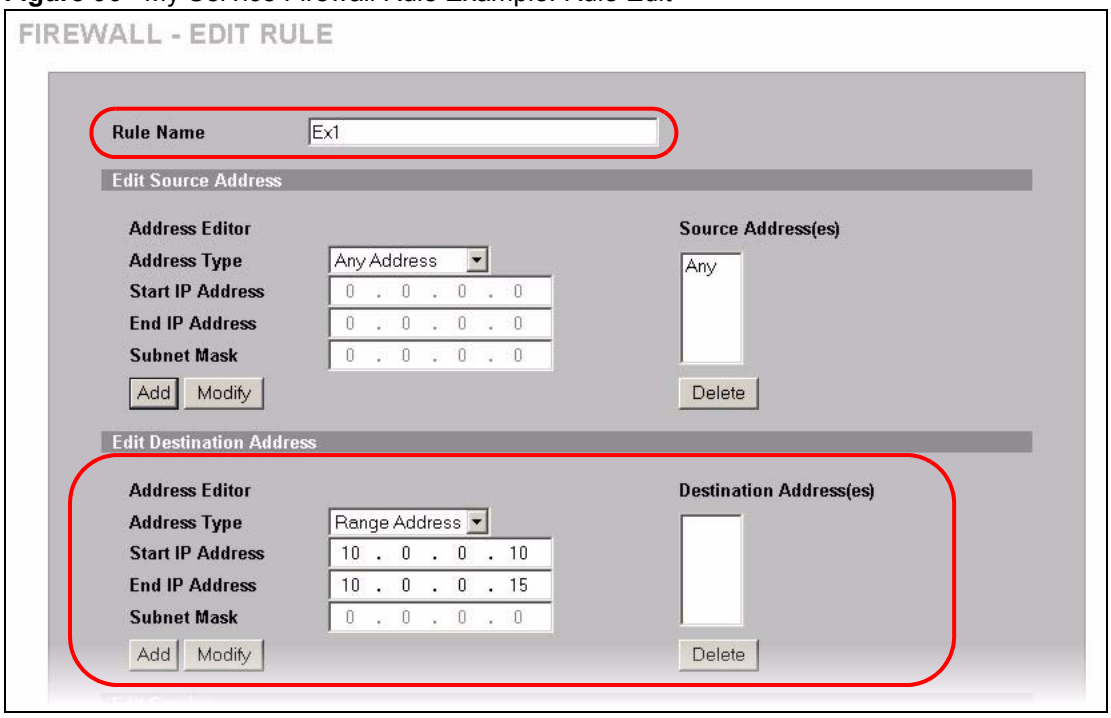

FIREWALL
Default Rule
Rule Summary
Anti-Probing
Threshold
Service
Rule Summary
Packet Direction: WAN To LAN Refresh
Name Active Source Address Destination Address Service Type Action Sch. Log Modify
WAN to LAN - Default Policy : Drop
1 W2L_Rule_1 N Any Any BOOTP_CLIENT(UDP:68) Permit No No
2 W2L_Rule_2 N Any Any NetBIOS(TCP/UDP:137~139,445) Permit No No

6 Enter the name of the firewall rule.

7 Select **Any** in the **Destination Address(es)** box and then click **Delete**.

8 Configure the destination address fields as follows and click **Add**.

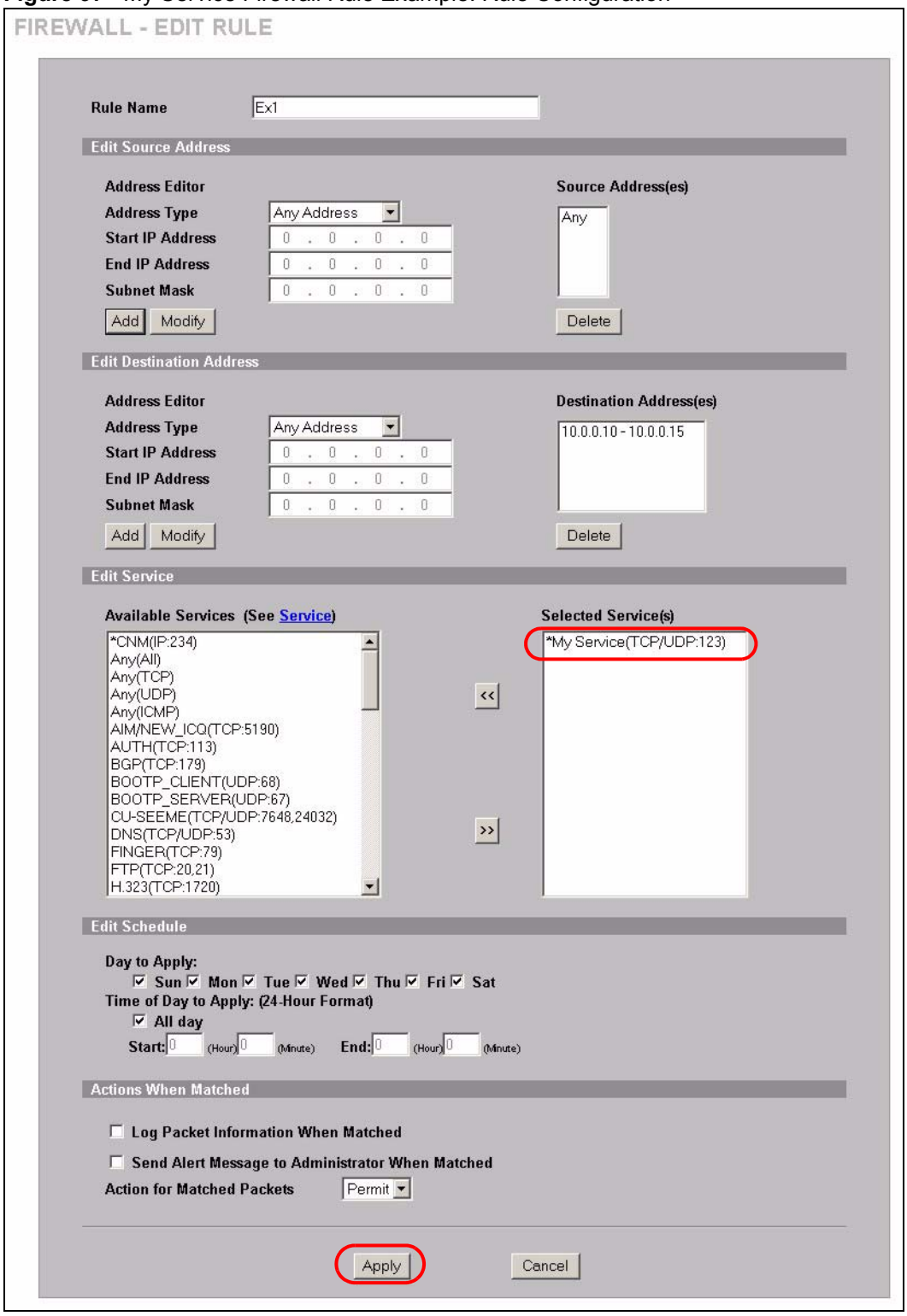
Figure 96 My Service Firewall Rule Example: Rule Edit



9 In the **Edit Rule** screen, use the arrows between **Available Services** and **Selected Service(s)** to configure it as follows. Click **Apply** when you are done.

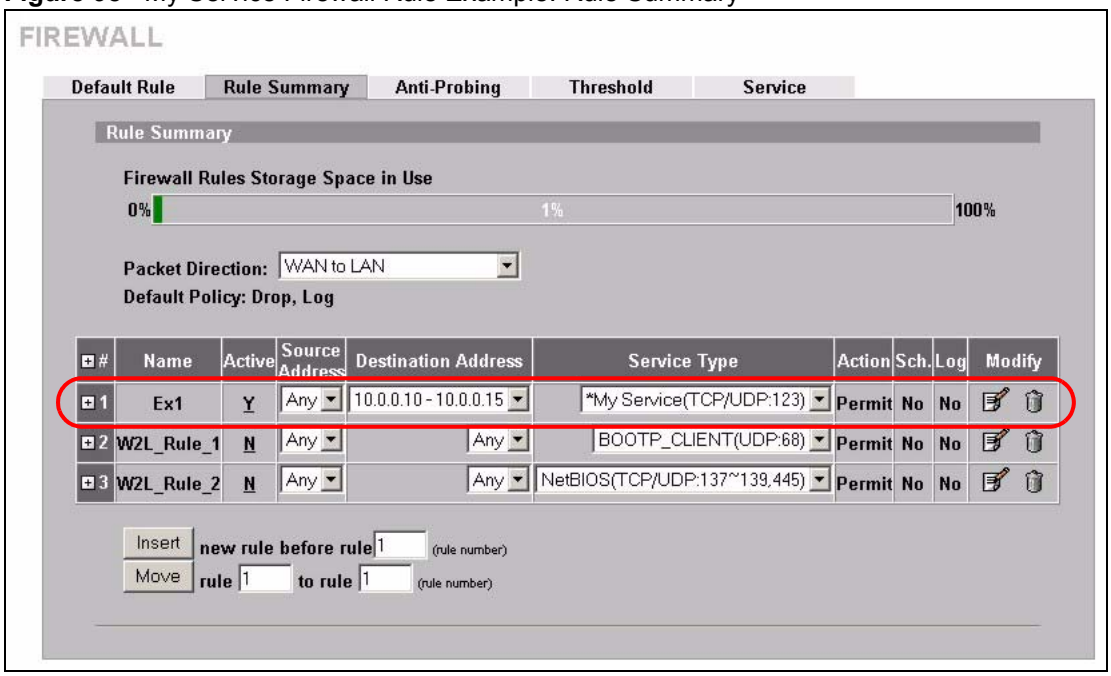
Custom services show up with an * before their names in the **Services** list box and the **Rule Summary** list box.

Figure 97 My Service Firewall Rule Example: Rule Configuration



Rule 1 allows a My Service connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

Figure 98 My Service Firewall Rule Example: Rule Summary


FIREWALL
Default Rule
Rule Summary
Anti-Probing
Threshold
Service
Rule Summary
Firewall Rules Storage Space in Use
0%
1%
100%
Packet Direction: WAN to LAN
Default Policy: Drop, Log
Name Active Source Address Destination Address Service Type Action Sch. Log Modify
1 Ex1 Y Any 10.0.0.10 - 10.0.0.15 *My Service(TCP/UDP:123) Permit No No
2 W2L_Rule_1 N Any Any BOOTP_CLIENT(UDP:68) Permit No No
3 W2L_Rule_2 N Any Any NetBIOS(TCP/UDP:137~139,445) Permit No No
Insert new rule before rule 1 (rule number)
Move rule 1 to rule 1 (rule number)

10

Intrusion Detection and Prevention (IDP)

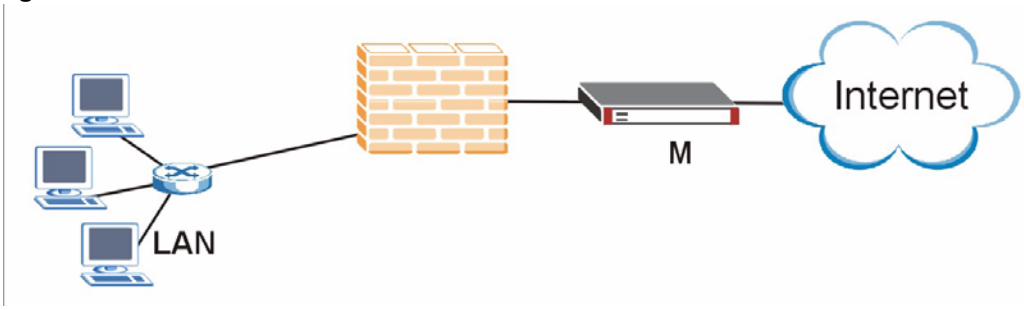
This chapter introduces some background information on IDP. Skip to the next chapter to see how to configure IDP on your ZyWALL.

10.1 Introduction to IDP

An IDP system can detect malicious or suspicious packets and respond instantaneously. It can detect anomalies based on violations of protocol standards (RFCs – Requests for Comments) or traffic flows and abnormal flows such as port scans.

Figure 99 on page 171 represents a typical business network consisting of a LAN containing web, FTP and mail servers, a firewall and/or NAT router connected to a broadband modem (M) for Internet access.

Figure 99 Network Intrusions



10.2 Firewalls and Intrusions

Firewalls are designed to block clearly suspicious traffic and forward other traffic through. Many exploits take advantage of weaknesses in the protocols that are allowed through the firewall, so that once an inside server has been compromised it can be used as a backdoor to launch attacks on other servers.

Firewalls are usually deployed at the network edge. However, many attacks (inadvertently) are launched from within an organization. Virtual private networks (VPN), removable storage devices and wireless networks may all provide access to the internal network without going through the firewall.

10.3 IDS and IDP

An Intrusion Detection System (IDS) can detect suspicious activity, but does not take action against attacks. On the other hand an IDP is a proactive defense mechanisms designed to detect malicious packets within normal network traffic and take an action (block, drop, log, send an alert) against the offending traffic automatically before it does any damage. An IDS only raises an alert after the malicious payload has been delivered. Worms such as Slammer and Blaster have such fast proliferation speeds that by the time an alert is generated, the damage is already done and spreading fast.

There are two main categories of IDP; Host IDP and Network IDP.

10.4 Host IDP

The goal of host-based intrusions is to infiltrate files on an individual computer or server in with the goal of accessing confidential information or destroying information on a computer.

You must install Host IDP directly on the system being protected. It works closely with the operating system, monitoring and intercepting system calls to the kernel or APIs in order to prevent attacks as well as log them.

Disadvantages of host IDPs are that you have to install them on each device (that you want to protect) in your network and due to the necessarily tight integration with the host operating system, future operating system upgrades could cause problems.

10.5 Network IDP

Network-based intrusions have the goal of bringing down a network or networks by attacking computer(s), switch(es), router(s) or modem(s). If a LAN switch is compromised for example, then the whole LAN is compromised, resulting in the equivalent of a LAN Denial of Service (DoS) attack. Host-based intrusions may be used to cause network-based intrusions when the goal of the host virus is to propagate attacks on the network, or attack computer/server operating system vulnerabilities with the goal of bringing down the computer/server. Typical "network-based intrusions" are SQL slammer, Blaster, Nimda, MyDoom etc.

A Network IDP has at least two network interfaces, one internal and one external. As packets appear at an interface they are passed to the detection engine, which determines whether they are malicious or not. If a malicious packet is detected, an action is taken. The remaining packets that make up that particular TCP session are also discarded.

10.6 Example Intrusions

The following are some examples of intrusions.

10.6.1 SQL Slammer Worm

W32.SQLExp.Worm is a worm that targets the systems running Microsoft SQL Server 2000, as well as Microsoft Desktop Engine (MSDE) 2000. The worm sends 376 bytes to UDP port 1434, the SQL Server Resolution Service Port. The worm has the unintended payload of performing a Denial of Service attack due to the large number of packets it sends. Refer to Microsoft SQL Server 2000 or MSDE 2000 vulnerabilities in *Microsoft Security Bulletin MS02-039* and *Microsoft Security Bulletin MS02-061*.

10.6.2 Blaster W32.Worm

This is a worm that exploits the DCOM RPC vulnerability (see *Microsoft Security Bulletin MS03-026* and *Microsoft Security Bulletin MS03-039*) using TCP port 135. The worm targets only Windows 2000 and Windows XP machines. While Windows NT and Windows 2003 Server machines are vulnerable (if not properly patched), the worm is not coded to replicate on those systems. This worm attempts to download the msblast.exe file to the %WinDir%\system32 directory and then execute it. W32.Blaster.Worm does not mass mail to other devices.

10.6.3 Nimda

Its name (backwards for "admin") refers to an "admin.DLL" file that, when run, continues to propagate the virus. Nimda probes each IP address within a randomly selected range of IP addresses, attempting to exploit weaknesses that, unless already patched, are known to exist in computers with Microsoft's Internet Information Server. A system with an exposed IIS Web server will read a Web page containing an embedded JavaScript that automatically executes, causing the same JavaScript code to propagate to all Web pages on that server. As Microsoft Internet Explorer browsers version 5.01 or earlier visit sites at the infected Web server, they unwittingly download pages with the JavaScript code that automatically executes, causing the virus to be sent to other computers on the Internet in a somewhat random fashion. Nimda also can infect users within the Web server's own internal network that have been given a network share (a portion of file space). Finally, one of the things that Nimda has an infected system do is to send an e-mail with a "readme.exe" attachment to the addresses in the local Windows address book. A user who opens or previews this attachment (which is a Web page with the JavaScript) propagates the virus further.

Server administrators should get and apply the cumulative IIS patch that Microsoft has provided for previous viruses and ensure that no one at the server opens e-mail. You should update your Internet Explorer version to IE 5.5 SP2 or later. Scan and cleanse your system with anti-virus software.

10.6.4 MyDoom

MyDoom W32.Mydoom.A@mm (also known as W32.Novarg.A) is a mass-mailing worm that arrives as an attachment with an bat, cmd, exe, pif, scr, or zip file extension. When a computer is infected, the worm sets up a backdoor into the system by opening TCP ports 3127 through 3198, which can potentially allow an attacker to connect to the computer and use it as a proxy to gain access to its network resources. In addition, the backdoor can download and execute arbitrary files. Systems affected are Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP and Windows Server 2003.

W32/MyDoom-A is a worm that is spread by email. When the infected attachment is launched, the worm gathers e-mail addresses from address books and from files with the following extensions: WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB and PL. W32/MyDoom-A creates a file called Message in the temp folder and runs Notepad to display the contents, which displays random characters. W32/MyDoom-A creates randomly chosen email addresses in the "To:" and "From:" fields as well as a randomly chosen subject line. Attached files will have an extension of BAT, CMD, EXE, PIF, SCR or ZIP.

10.7 ZyWALL IDP

The ZyWALL Internet Security Appliance is designed to protect against network-based intrusions. See Section 11.2 on page 175 for more information on how to apply IDP to ZyWALL interfaces.

IDP is regularly updated by the ZyXEL Security Response Team (ZSRT). Regular updates are vital as new intrusions evolve.

11

Configuring IDP

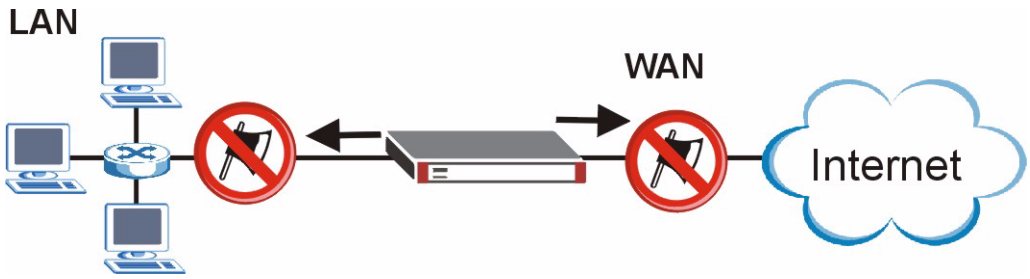
This chapter shows you how to configure IDP on the ZyWALL.

11.1 Overview

Intrusion Detection and Prevention (IDP) checks traffic going out from the ZyWALL to the interface(s) you specify for signature matches.

If a packet matches a signature, the action specified by the signature is taken. You can change the default signature actions in the **Signatures** screen.

Figure 100 Applying IDP to Interfaces

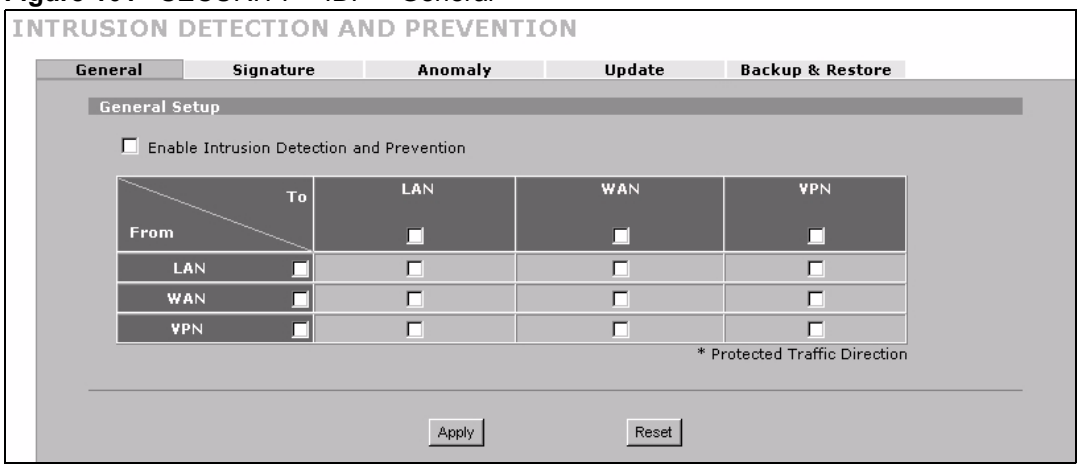


11.2 General Setup

Use this screen to enable IDP on the ZyWALL and choose what interface(s) you want to protect from intrusions.

Click **SECURITY > IDP** from the navigation panel. **General** is the first screen as shown in the following figure.

Figure 101 SECURITY > IDP > General



The following table describes the labels in this screen.

Table 47 SECURITY > IDP > General Setup

LABEL	DESCRIPTION
General Setup	
Enable Intrusion Detection and Protection	Select this check box to enable IDP on the ZyWALL. When this check box is cleared the ZyWALL is in IDP "bypass" mode and no IDP checking is done.
From, To	Select the directions of travel of packets that you want to check. Select or clear a row or column's first check box (with the interface label) to select or clear the interface's whole row or column. For example, **From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the ZyWALL or the ZyWALL itself. The ZyWALL does not check packets traveling from a LAN computer to another LAN computer on the same subnet. **From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN or terminating at the ZyWALL's LAN interface. The ZyWALL checks the traffic after decrypting it. **To VPN** is traffic that comes in through the selected "from" interface and goes out through the VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through the VPN tunnel. The ZyWALL checks the traffic before encrypting it. **From VPN To VPN** means traffic that comes in through the VPN tunnel and terminates at the ZyWALL. This is the case if you allow someone to use a service (like Telnet or HTTP) through the VPN tunnel to manage the ZyWALL. The ZyWALL checks the traffic after decrypting it (before encrypting it again). Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnel. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic).
Protected Interface	Select the **Active** check box to apply IDP to the corresponding interface. Traffic going from the ZyWALL out through this interface is then checked against the signature database for possible intrusions. For example, if you want to protect the LAN computers from intrusions, select the **LAN** interface.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

11.3 IDP Signatures

The rules that define how to identify and respond to intrusions are called “signatures”. Click **SECURITY > IDP** > **Signatures** to see the ZyWALL’s signatures.

11.3.1 Attack Types

Click **SECURITY > IDP** > **Signature**. The **Attack Type** list box displays all intrusion types supported by the ZyWALL. **Other** covers all intrusion types not covered by other types listed.

To see signatures listed by intrusion type supported by the ZyWALL, select that type from the **Attack Type** list box.

Figure 102 SECURITY > IDP > Signatures: Attack Types

The following table describes each attack type.

Table 48 SECURITY > IDP > Signature: Attack Types

TYPE	DESCRIPTION
DoS/DDoS	The goal of Denial of Service (DoS) attacks is not to steal information, but to disable a device or network on the Internet. A distributed denial-of-service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.
Buffer Overflow	A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. The excess information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Intruders could run codes in the overflow buffer region to obtain control of the system, install a backdoor or use the victim to launch attacks on other devices.
Access Control	Access control refers to procedures and controls that limit or detect access. Access control is used typically to control user access to network resources such as servers, directories, and files.
Scan	Scan refers to all port, IP or vulnerability scans. Hackers scan ports to find targets. They may use a TCP connect() call, SYN scanning (half-open scanning), Nmap etc. After a target has been found, a vulnerability scanner can be used to exploit exposures.
Trojan Horse	A Trojan horse is a harmful program that’s hidden inside apparently harmless programs or data. It could be used to steal information or remotely control a device.

Table 48 SECURITY > IDP > Signature: Attack Types (continued)

TYPE	DESCRIPTION
P2P	Peer-to-peer (P2P) is where computing devices link directly to each other and can directly initiate communication with each other; they do not need an intermediary. A device can be both the client and the server. In the ZyWALL, P2P refers to peer-to-peer applications such as eMule, eDonkey, BitTorrent, iMesh etc.
IM	IM (Instant Messaging) refers to chat applications. Chat is real-time communication between two or more users via networks-connected computers. After you enter a chat (or chat room), any member can type a message that will appear on the monitors of all the other participants.
Virus/Worm	A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a program that is designed to copy itself from one computer to another on a network. A worm's uncontrolled replication consumes system resources thus slowing or stopping other tasks. The IDP VirusWorm category refers to network-based viruses and worms. The Anti-Virus (AV) screen refers to file-based viruses and worms. Refer to the anti-virus chapter for additional information on file-based anti-virus scanning in the ZyWALL.
Porn	The ZyWALL can block web sites if their URLs contain certain pornographic words. It cannot block web pages containing those words if the associated URL does not.
Web Attack	Web attack signatures refer to attacks on web servers such as IIS (Internet Information Services).
SPAM	Spam is unsolicited "junk" e-mail sent to large numbers of people to promote products or services.
Other	This category refers to signatures for attacks that do not fall into the previously mentioned categories.

11.3.2 Intrusion Severity

Intrusions are assigned a severity level based on the following table. The intrusion severity level then determines the default signature action.

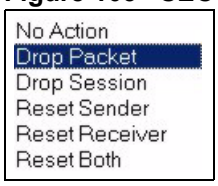
Table 49 SECURITY > IDP > Signature: Intrusion Severity

SEVERITY	DESCRIPTION
Severe	These are intrusions that try to run arbitrary code or gain system privileges.
High	These are known serious vulnerabilities or intrusions that are probably not false alarms.
Medium	These are medium threats, access control intrusions or intrusions that could be false alarms.
Low	These are mild threats or intrusions that could be false alarms.
Very Low	These are possible intrusions caused by traffic such as Ping, trace route, ICMP queries etc.

11.3.3 Signature Actions

You can enable/disable individual signatures. You can log and/or have an alert sent when traffic meets a signature criteria. You can also change the default action to be taken when a packet or stream matches a signature. The following figure and table describes these actions. Note that in addition to these actions, a log may be generated or an alert sent, if those check boxes are selected and the signature is enabled.

Figure 103 SECURITY > IDP > Signature: Actions



The following table describes signature actions.

Table 50 SECURITY > IDP > Signature: Actions

ACTION	DESCRIPTION
No Action	The intrusion is detected but no action is taken.
Drop Packet	The packet is silently discarded.
Drop Session	When the firewall is enabled, subsequent TCP/IP packets belonging to the same connection are dropped. Neither sender nor receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.
Reset Sender	When the firewall is enabled, the TCP/IP connection is silently torn down. Just the sender is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.
Reset Receiver	When the firewall is enabled, the TCP/IP connection is silently torn down. Just the receiver is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.
Reset Both	When the firewall is enabled, the TCP/IP connection is silently torn down. Both sender and receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.

11.3.4 Configuring IDP Signatures

Click **IDP** > **Signature** to see the ZyWALL's "group view" signature screen where you can view signatures by attack type. To search for signatures based on other criteria such as signature name or ID, then click the **Switch to query view** link to go to the "query view" screen.

You can take actions on these signatures as described in Section 11.3.3 on page 178. To revert to the default actions or to save sets of actions, go to the **Backup & Restore** screen.

Figure 104 SECURITY > IDP > Signature: Group View

The following table describes the labels in this screen.

Table 51 SECURITY > IDP > Signature: Group View

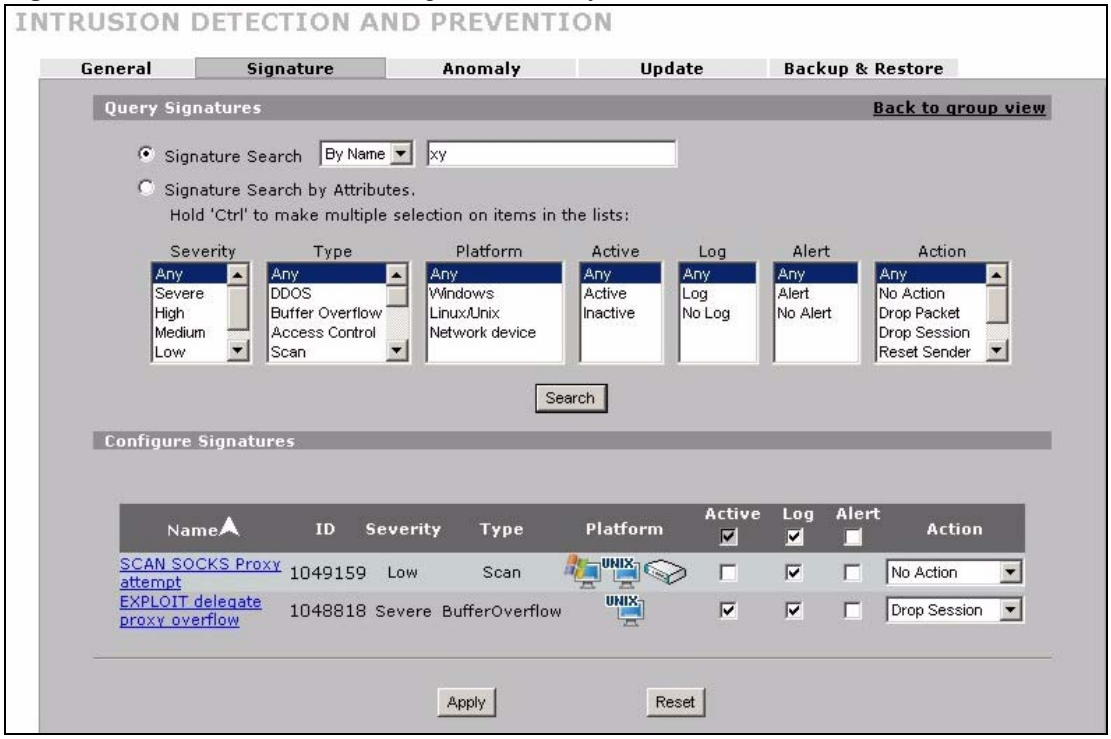
LABEL	DESCRIPTION
Signature Groups	
Switch to query view	Click this hyperlink to go to a screen where you can search for signatures based on criteria other than attack type.
Attack Type	Select the type of signatures you want to view from the list box. See Section 11.3.1 on page 177 for information on types of signatures. The table displays the signatures of the type that you selected. Click a column's header to sort the entries by that attribute.
Name	The (read-only) signature name identifies a specific signature targeted at a specific intrusion. Click the hyperlink for more detailed information on the intrusion.
ID	Each intrusion has a unique identification number. This number may be searched at myZyXEL.com for more detailed information.
Severity	This field displays the level of threat that the intrusion may pose. See Table 49 on page 178 for more information on intrusion severity.
Platform	This field displays the computer or network device operating system that the intrusion targets or is vulnerable to the intrusion. These icons represent a Windows operating system, a UNIX-based operating system and a network device respectively.
Active	Select the check box in the heading row to automatically select all check boxes and enable all signatures. Clear it to clear all entries and disable all signatures on the current page. For example, you could clear all check boxes for signatures that targets operating systems not in your network. This would speed up the IDP signature checking process. Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box. If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared).
Log	Select this check box to have a log generated when a match is found for a signature. Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page. Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box. If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared).
Alert	You can only edit the **Alert** check box when the corresponding **Log** check box is selected. Select this check box to have an e-mail sent when a match is found for a signature. Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page. Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box. If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared).
Action	You can change the default signature action here. See Table 50 on page 179 for more details on actions.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

11.3.5 Query View

Click **IDP** > **Signature** to see the ZyWALL's "group view" signature screen, then click the **Switch to query view** link to go to this 'query view" screen.

Use this screen to search for signatures by criteria such as name, ID, severity, attack type, vulnerable attack platforms, whether or not they are active, log options, alert options or actions.

Figure 105 SECURITY > IDP > Signature: Query View



The following table describes the fields in this screen.

Table 52 SECURITY > IDP > Signature: Query View

LABEL	DESCRIPTION
Back to group view	Click this button to go to the IDP group view screen where IDP signatures are grouped by attack type.
Signature Search	Select this to search for a specific signature name or ID (that you already know). Then select whether to search the signatures by name or ID. Then enter the name (or part of the name) or the complete ID number of the signature(s) that you want to find.
Signature Search by Attributes	Select this to search for signatures that match the criteria that you specify. Then select the criteria to search for. Hold down the [Ctrl] key if you want to make multiple selections from a list of attributes.
Severity	Search for signatures by severity level(s) (see Table 49 on page 178).
Type	Search for signatures by attack type(s) (see Table 48 on page 177). Attack types are known as policy types in the group view screen.
Platform	Search for signatures created to prevent intrusions targeting specific operating system(s).
Active	Search for enabled and/or disabled signatures here.

Table 52 SECURITY > IDP > Signature: Query View (continued)

LABEL	DESCRIPTION
Log	Search for signatures by log option here.
Alert	Search for signatures by alert option here.
Action	Search for signatures by the response the ZyWALL takes when a packet matches a signature. See Table 50 on page 179 for action details.
Search	Click this button to begin the search. The results display at the bottom of the screen. Results may be spread over several pages depending on how broad the search criteria selected were. The tighter the criteria selected, the fewer the signatures returned.
Configure Signatures	The results display in a table showing the criteria as selected in the search. Click a column's header to sort the entries by that attribute.
Go To Page	Navigate between pages of signatures found.
Name	The (read-only) signature name identifies a specific signature targeted at a specific intrusion. Click the hyperlink for more detailed information on the intrusion.
ID	Each intrusion has a unique identification number. This number may be searched at myZyXEL.com for more detailed information.
Severity	This field displays the level of threat that the intrusion may pose. See Table 49 on page 178 for more information on intrusion severity.
Platform	This field displays the computer or network device operating system that the intrusion targets or is vulnerable to the intrusion. These icons represent a Windows operating system, a UNIX-based operating system and a network device respectively.
Active	Select the check box in the heading row to automatically select all check boxes and enable all signatures. Clear it to clear all entries and disable all signatures on the current page. For example, you could clear all check boxes for signatures that targets operating systems not in your network. This would speed up the IDP signature checking process. Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box. If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared).
Log	Select this check box to have a log generated when a match is found for a signature. Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page. Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box. If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared).

Table 52 SECURITY > IDP > Signature: Query View (continued)

LABEL	DESCRIPTION
Alert	You can only edit the **Alert** check box when the corresponding **Log** check box is selected. Select this check box to have an e-mail sent when a match is found for a signature. Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page. Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box. If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared).
Action	You can change the default signature action here. See Table 50 on page 179 for more details on actions.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

11.3.5.1 Query Example 1

1 From the "group view" signature screen, click the **Switch to query view** link.

1 Select **Signature Search**.

2 Select **By Name** or **By ID** from the list box.

3 Enter a name (complete or partial) or complete ID to display all relevant signatures in the signature database.

A partial name may be searched but a complete ID number must be entered before a match can be found. For example, a search by name for "w" (in the first example) finds all intrusions that contain this letter in the name field. However a search by ID for "1" would return no match. You must enter the complete ID as shown in the second example.

4 Click **Search**. If the search finds more signatures than can be displayed on one page, use the **Go to Page** list box to view other pages of signatures found in the search.

5 If you change the **Active**, **Log**, **Alert** and/or **Action** signature fields in the signatures found, then click **Apply** to save the changes to the ZyWALL.

Figure 106 SECURITY > IDP > Signature: Query by Partial Name

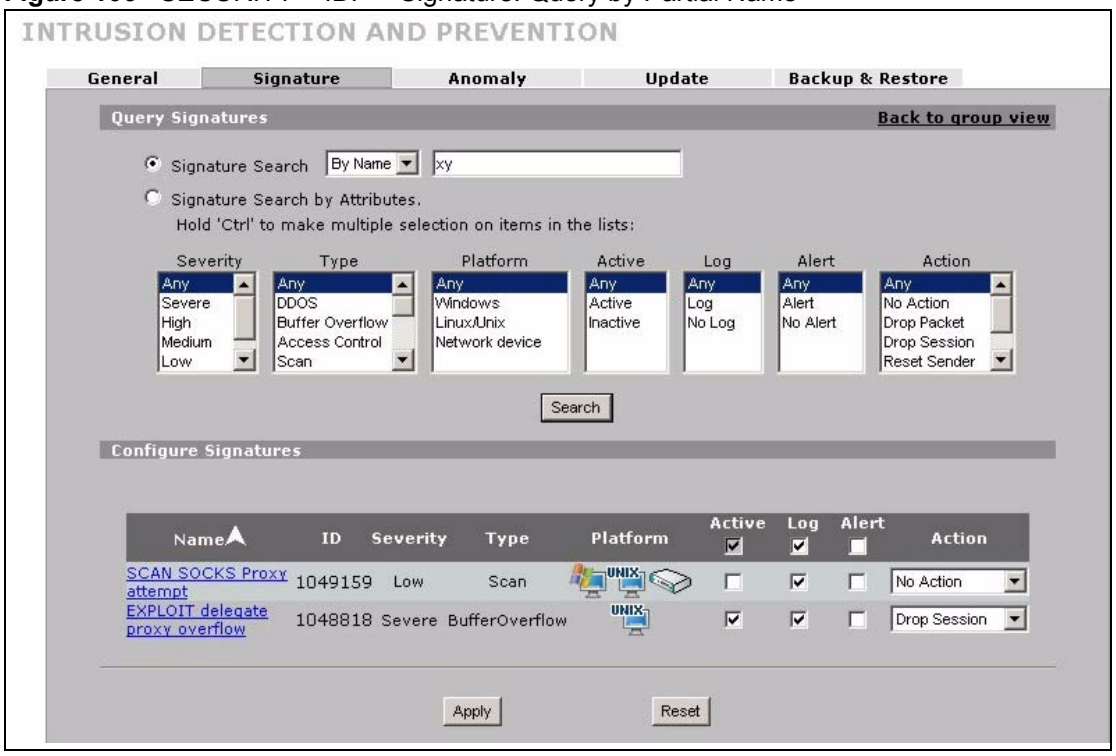


Figure 107 SECURITY > IDP > Signature: Query by Complete ID

11.3.5.2 Query Example 2

1 From the "group view" signature screen, click the **Switch to query view** link.

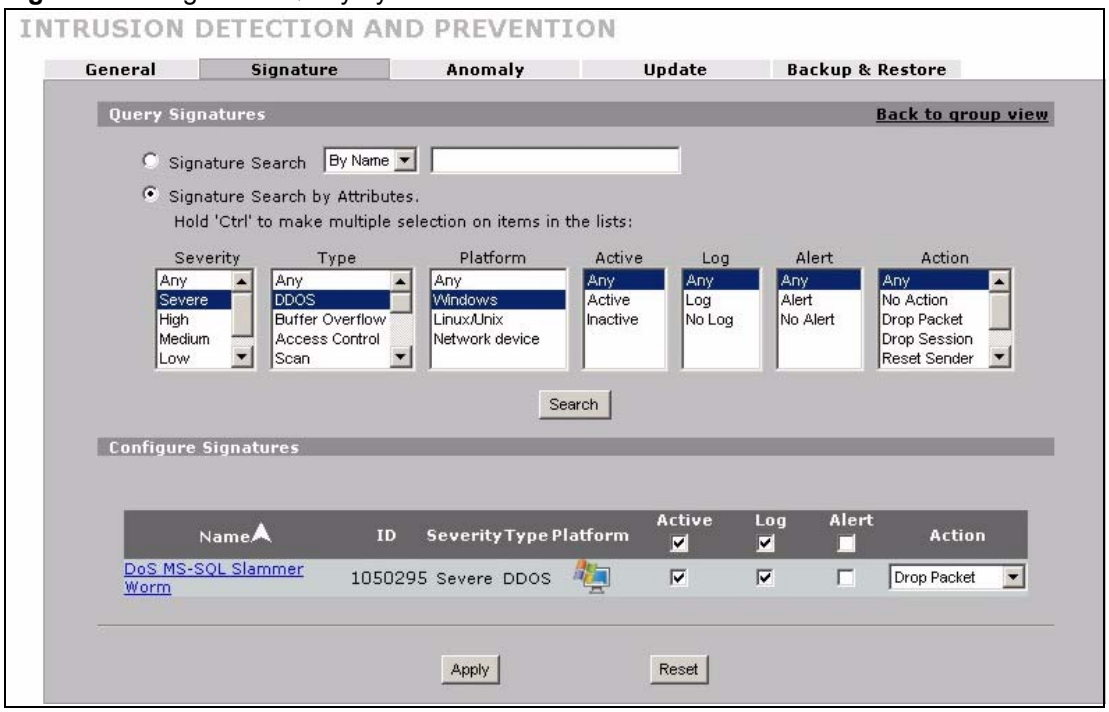
1 Select **Signature Search By Attributes**.

2 Select the **Severity**, **Type**, **Platform**, **Active**, **Log**, **Alert** and/or **Action** items. In this example all severe **DDoS** type signatures that target the Windows operating system are displayed.

3 Click **Search**.

If you change the **Active**, **Log**, **Alert** and/or **Action** signature fields in the signatures found, then click **Apply** to save the changes to the ZyWALL.

Figure 108 Signature Query by Attribute.

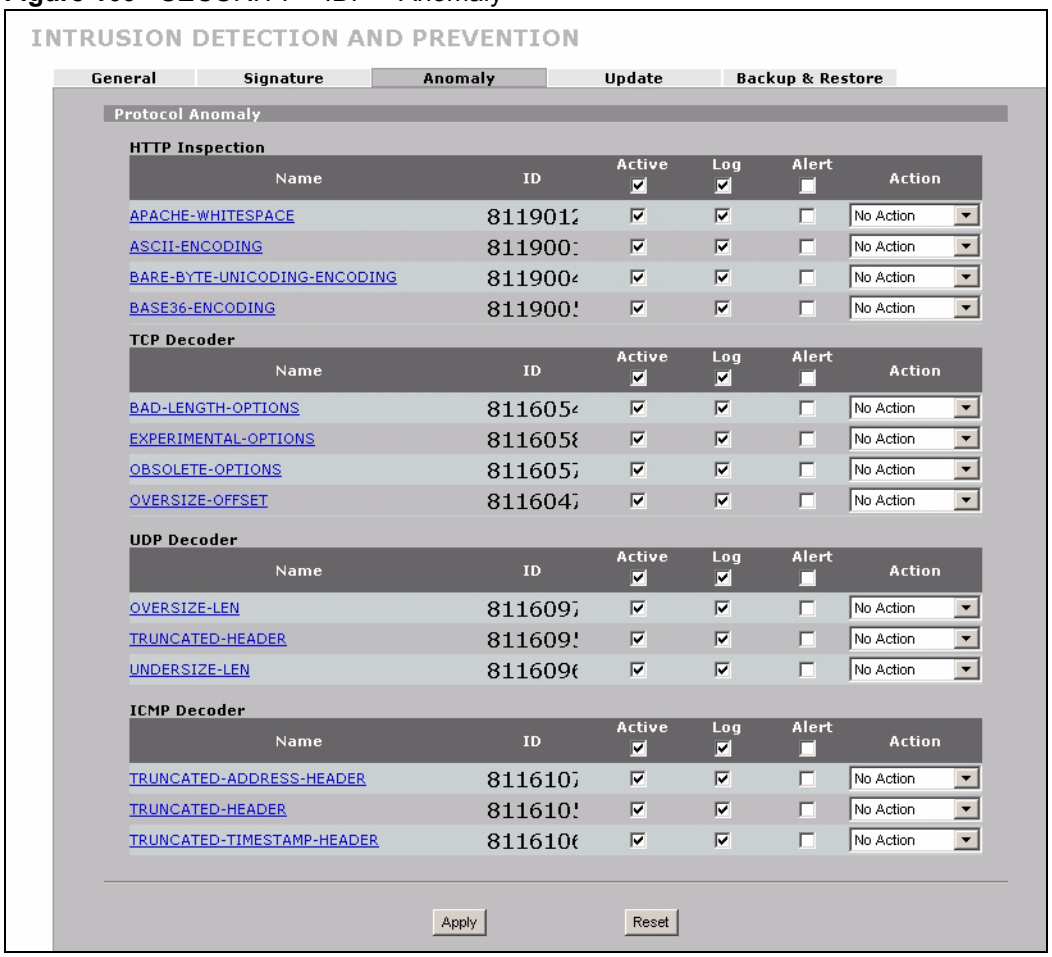


11.4 Anomaly

This section introduces ADP (Anomaly Detection and Prevention). An ADP system protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal flows such as port scans. Protocol anomaly detection includes HTTP Inspection, TCP Decoder, UDP Decoder and ICMP Decoder. Protocol anomaly rules may be updated when you upload new firmware.

Click **SECURITY > IDP > Anomaly** to display the following screen.

Figure 109 SECURITY > IDP > Anomaly



The following table describes the labels in this screen.

Table 53 SECURITY > IDP > Anomaly

LABEL	DESCRIPTION
Protocol Anomaly	
HTTP Inspection/TCP Decoder/UDP Decoder/ICMP Decoder	
Name	This is the name of the protocol anomaly rule. Click a name to display more detailed information on a rule.
ID	This is the unique identifying number for the anomaly rule.
Active	Select the head of the **Active** column to activate all rules for an anomaly detection method, or select **Active** for an individual rule to make it active.
Log	Select the head of the **Log** column to generate logs for all rules included in an anomaly detection method. Select **Log** to generate a log when a match is found for the corresponding rule. See Chapter 23 on page 351 for more information on logs.
Alert	Select the head of the **Alert** column to activate the alert for all rules in an anomaly detection method. Select **Alert** to generate an alert log when a match is found for the corresponding rule. See Chapter 23 on page 351 for more information on alerts.

Table 53 SECURITY > IDP > Anomaly (continued)

LABEL	DESCRIPTION
Action	Select what the ZyWALL should do when a packet matches a rule. **No Action**: The ZyWALL takes no action when a packet matches the signature(s). **Drop Packet**: The packet is silently discarded. **Drop Session**: When the firewall is enabled, subsequent TCP/IP packets belonging to the same connection are dropped. Neither sender nor receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. **Reset Sender**: When the firewall is enabled, the TCP/IP connection is silently torn down. Just the sender is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. **Reset Receiver**: When the firewall is enabled, the TCP/IP connection is silently torn down. Just the receiver is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. **Reset Both**: When the firewall is enabled, the TCP/IP connection is silently torn down. Both sender and receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.
Apply	Click this button to save your changes.
Reset	Click this button to begin configuring this screen afresh.

11.5 Update

The ZyWALL comes with built-in signatures created by the ZyXEL Security Response Team (ZSRT). These are regularly updated as new intrusions evolve. Use the **Update** screen to immediately download or schedule new signature downloads.

You should have already registered the ZyWALL at myZyXEL.com (http://www.myzyxel.com/myzyxel/) and also have either activated the trial license or standard license (iCard). If your license has expired, you will have to renew it before updates are allowed.

11.5.1 mySecurityZone

mySecurityZone is a web portal that provides all security-related information such as intrusion and anti-virus information for ZyXEL security products.

Click the intrusion **ID** hyperlink to go directly to information on that signature or enter https://mysecurity.zyxel.com/mysecurity/ as the URL in your web browser.

You should have already registered your ZyWALL on myZyXEL.com at:

http://www.myzyxel.com/myzyxel/.

You can use your myZyXEL.com username and password to log into mySecurityZone.

11.5.2 Configuring IDP Update

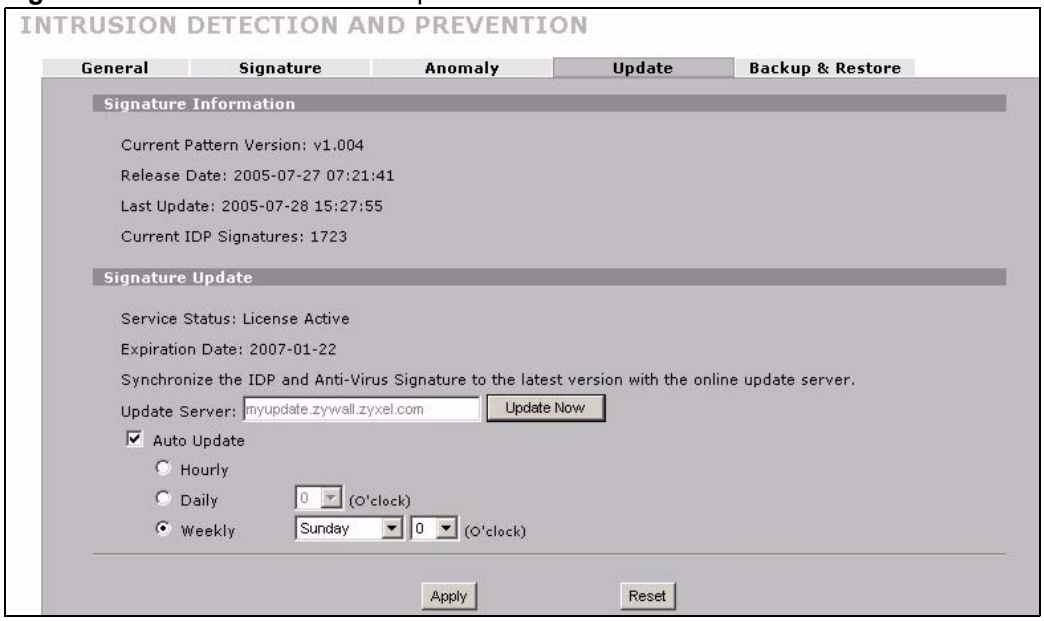
When scheduling signature updates, you should choose a day and time when your network is least busy so as to minimize disruption to your network. Your custom signature configurations are not over-written when you download new signatures.

File-based anti-virus signatures (see the anti-virus chapter) are included with IDP signatures. When you download new signatures using the anti-virus **Update** screen, IDP signatures are also downloaded. The version number changes both in the anti-virus **Update** screen and this screen. Both screens also share the same **Auto-Update** schedule. Changes made to the schedule in one screen are reflected in the other.

The ZyWALL does not have to reboot when you upload new signatures.

Click **SECURITY > IDP** > **Update**.

Figure 110 SECURITY > IDP > Update



The following table describes the labels in this screen.

Table 54 SECURITY > IDP > Update

LABEL	DESCRIPTION
Signature Information	
Current Pattern Version	This field displays the signatures version number currently used by the ZyWALL. This number is defined by the ZyXEL Security Response Team (ZSRT) who maintain and update them. This number increments as new signatures are added, so you should refer to this number regularly. Go to https://mysecurity.zyxel.com/mysecurity/ to see what the latest version number is. You can also subscribe to signature update e-mail notifications.
Release Date	This field displays the time (hour, minutes second) and date (month, date, year) that the above signature set was created.

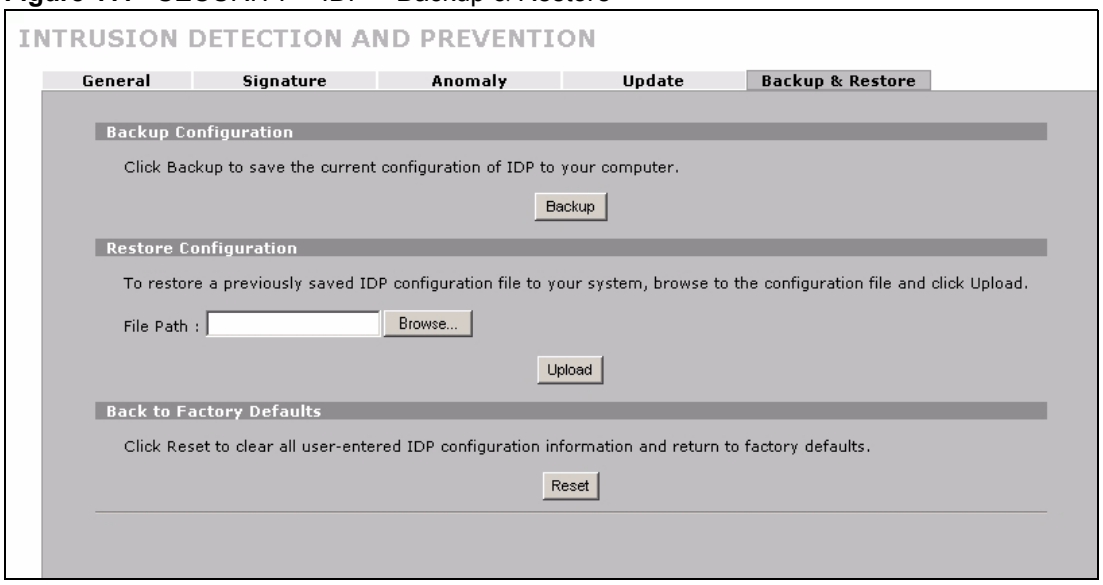
Table 54 SECURITY > IDP > Update (continued)

LABEL	DESCRIPTION
Last Update	This field displays the last date and time you downloaded new signatures to the ZyWALL. It displays **N/A** if you have not downloaded any new signatures yet.
Current IDP Signatures	This field displays the number of IDP-related signatures.
Signature Update	
Service Status	This field displays **License Inactive** if you have not yet activated your trial or iCard license at myZyXEL.com. It displays **License Inactive** and an expiration date if your trial or iCard license has expired (the expiration date is the date it expired). It displays **Trial Active** and an expiration date when you have activated your trial license. It displays **License Active** and an expiration date when you have activated your iCard license (the expiration date is the date it will expire).
Update Server	This is the URL of the signature server from which you download signatures.
Update Now	Click this button to begin downloading signatures from the **Update Server** immediately.
Auto Update	Select the check box to configure a schedule for automatic signature updates. The **Hourly**, **Daily** and **Weekly** fields display when the check box is selected. The ZyWALL then automatically downloads signatures from the **Update Server** regularly at the time and/or day you specify.
Hourly	Select this option to have the ZyWALL check the update server for new signatures every hour. This may be advisable when new intrusions are currently spreading throughout the Internet.
Daily	Select this option to have the ZyWALL check the update server for new signatures every day at the hour you select from the list box. The ZyWALL uses a 24-hour clock. For example, choose 15 from the **O'clock** list box to have the ZyWALL check the update server for new signatures at 3 PM every day.
Weekly	Select this option to have the ZyWALL check the update server for new signatures once a week on the day and hour you select from the list boxes. The ZyWALL uses a 24-hour clock, so for example, choose **Wednesday** and 15 from the respective list boxes to have the ZyWALL check the update server for new signatures at 3PM every Wednesday.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to close this screen without saving any changes.

11.6 Backup and Restore

You can change the pre-defined Active, Log, Alert and/or Action settings of individual signatures.

Figure 111 SECURITY > IDP > Backup & Restore


INTRUSION DETECTION AND PREVENTION
General
Signature
Anomaly
Update
Backup & Restore
Backup Configuration
Click Backup to save the current configuration of IDP to your computer.
Backup
Restore Configuration
To restore a previously saved IDP configuration file to your system, browse to the configuration file and click Upload.
File Path :
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered IDP configuration information and return to factory defaults.
Reset

Use the **Backup & Restore** screen to:

- Back up IDP signatures with your custom configured settings. Click **Backup** and then choose a location and filename for the IDP configuration set.
- Restore previously saved IDP signatures (with your custom configured settings). Click **Restore** and choose the path and location where the previously saved file resides on your computer.
- Revert to the original ZSRT-defined signature **Active**, **Log**, **Alert** and/or **Action** settings. Click **Reset**.

12

Anti-Virus

This chapter introduces and shows you how to configure the anti-virus scanner.

12.1 Anti-Virus Overview

A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a self-replicating virus that resides in active memory and duplicates itself. The effect of a virus attack varies from doing so little damage that you are unaware your computer is infected to wiping out the entire contents of a hard drive to rendering your computer inoperable.

12.1.1 Types of Computer Viruses

The following table describes some of the common computer viruses.

Table 55 Common Computer Virus Types

TYPE	DESCRIPTION
File Infector	This is a small program that embeds itself in a legitimate program. A file infector is able to copy and attach itself to other programs that are executed on an infected computer.
Boot Sector Virus	This type of virus infects the area of a hard drive that a computer reads and executes during startup. The virus causes computer crashes and to some extend renders the infected computer inoperable.
Macro Virus	Macro viruses or Macros are small programs that are created to perform repetitive actions. Macros run automatically when a file to which they are attached is opened. Macros spread more rapidly than other types of viruses as data files are often shared on a network.
E-mail Virus	E-mail viruses are malicious programs that spread through e-mail.
Polyrmorphic Virus	A polymorphic virus (also known as a mutation virus) tries to evade detection by changing a portion of its code structure after each execution or self replication. This makes it harder for an anti-virus scanner to detect or intercept it. A polymorphic virus can also belong to any of the virus types discussed above.

12.1.2 Computer Virus Infection and Prevention

The following describes a simple life cycle of a computer virus.

1. A computer gets a copy of a virus from a source such as the Internet, e-mail, file sharing or any removable storage media. The virus is harmless until the execution of an infected program.
2. The virus spreads to other files and programs on the computer.

3 The infected files are unintentionally sent to another computer thus starting the spread of the virus.
4 Once the virus is spread through the network, the number of infected networked computers can grow exponentially.

12.1.3 Types of Anti-Virus Scanner

The section describes two types of anti-virus scanner: host-based and network-based.

A host-based anti-virus (HAV) scanner is often software installed on computers and/or servers in the network. It inspects files for virus patterns as they are moved in and out of the hard drive. However, host-based anti-virus scanners cannot eliminate all viruses for a number of reasons:

- HAV scanners are slow in stopping virus threats through real-time traffic (such as from the Internet).
- HAV scanners may reduce computing performance as they also share the resources (such as CPU time) on the computer for file inspection.
- You have to update the virus signatures and/or perform virus scans on all computers in the network regularly.

A network-based anti-virus (NAV) scanner is often deployed as a dedicated security device (such as your ZyWALL) on the network edge. NAV scanners inspect real-time data traffic (such as E-mail messages or web) that tends to bypass HAV scanners. The following lists some of the benefits of NAV scanners.

- NAV scanners stops virus threats at the network edge before they enter or exit a network.
- NAV scanners reduce computing loading on computers as the read-time data traffic inspection is done on a dedicated security device.

12.2 Introduction to the ZyWALL Anti-Virus Scanner

The ZyWALL has a built-in signature database. Setting up the ZyWALL between your local network and the Internet allows the ZyWALL to scan files transmitting through the enabled interfaces into your network. As a network-based anti-virus scanner, the ZyWALL helps stop threats at the network edge before they reach the local host computers.

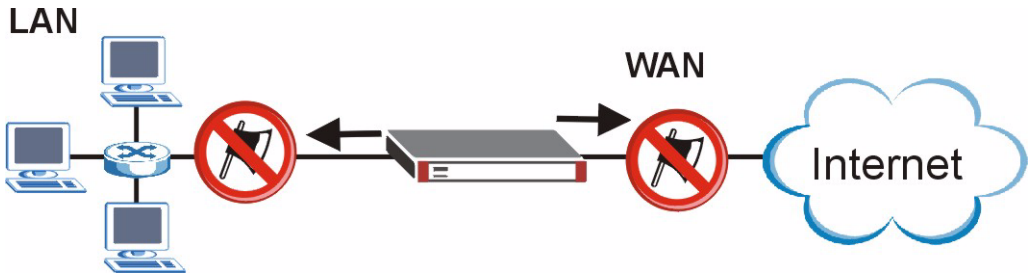
You can set the ZyWALL to examine files received through the following protocols:

- FTP (File Transfer Protocol)
- HTTP (Hyper Text Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- POP3 (Post Office Protocol version 3)

12.2.1 How the ZyWALL Anti-Virus Scanner Works

The ZyWALL checks traffic going to the interface(s) you specify for signature matches.

Figure 112 ZyWALL Anti-virus Example



The following describes the virus scanning process on the ZyWALL.

1. The ZyWALL first identifies SMTP, POP3, HTTP and FTP packets through standard ports.
2. If the packets are not session connection setup packets (such as SYN, ACK and FIN), the ZyWALL records the sequence of the packets.
3. The scanning engine checks the contents of the packets for virus.
4. If a virus pattern is matched, the ZyWALL "destroys" the file by removing the infected portion of the file.
5. If the send alert message function is enabled, the ZyWALL sends an alert to the file's indented destination computer(s).

Since the ZyWALL erases the infected portion of the file before sending it, you may not be able to open the file.

12.2.2 Notes About the ZyWALL Anti-Virus

1. The ZyWALL anti-virus scanner cannot detect polymorphic viruses.
2. When a virus is detected, an alert message is displayed in Microsoft Windows computers.[1]
3. The ZyWALL does not scan the following file/traffic types:
   - Simultaneous downloads of a file using multiple connections. For example, when you use FlashGet to download sections of a file simultaneously.
   - Encrypted traffic (such as on a VPN) or password-protected files.
   - Traffic through custom (none-standard) ports.
   - ZIP file(s) within a ZIP file.

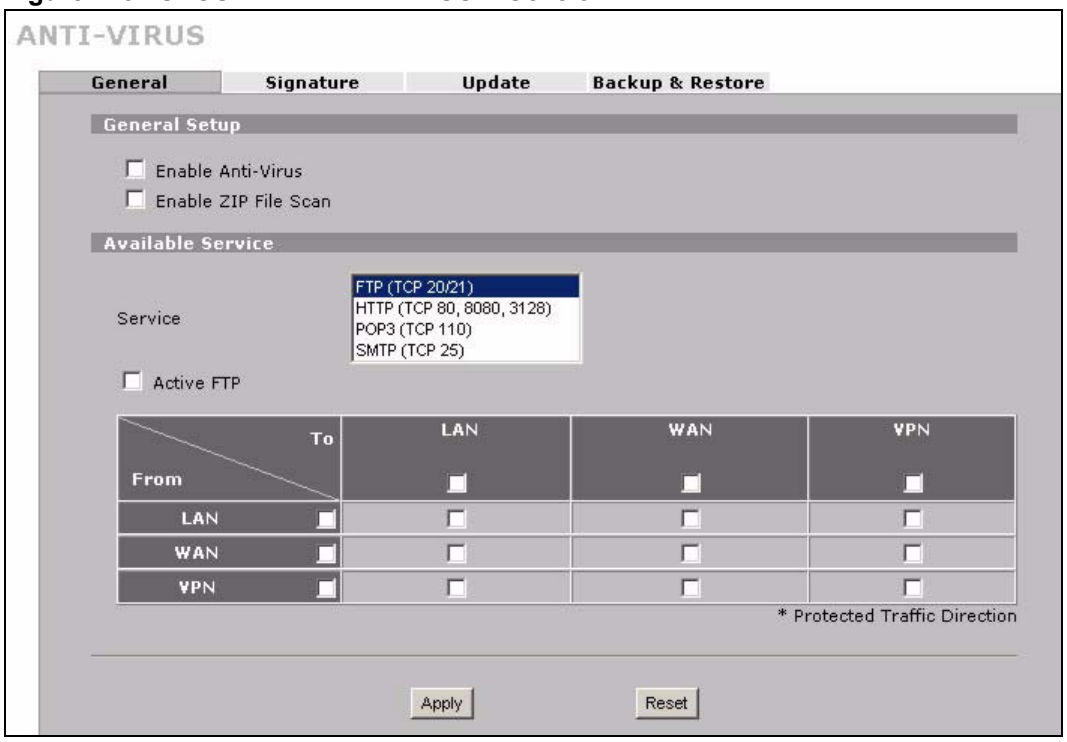
12.3 General Anti-Virus Setup

Click **SECURITY** > **ANTI-VIRUS** to display the configuration screen as shown next.

1. For Windows 98/Me, refer to the Appendix E on page 467 for requirements.

Before you use the anti-virus feature, you must register for the service (refer to the chapter on registration for more information).

Figure 113 SECURITY > ANTI-VIRUS > General



The following table describes the labels in this screen.

Table 56 SECURITY > ANTI-VIRUS > General

LABEL	DESCRIPTION
General Setup	
Enable Anti-Virus	Select this check box to check traffic for viruses.
Enable ZIP File Scan	Select this check box to have the ZyWALL scan a ZIP file (with the “zip”, “gzip” or “gz” file extension). The ZyWALL first decompresses the ZIP file and then scans the contents for viruses. Note: The ZyWALL decompresses a ZIP file once. The ZyWALL does NOT decompress any ZIP file(s) within the ZIP file.
Available Service	
Service	This field displays the services for which the ZyWALL can scan traffic for viruses. Select a service to be able to enable or disabled anti-virus scanning on it’s traffic. Here are the services and default port numbers. FTP traffic using TCP ports 20 and 21 HTTP traffic using TCP ports 80, 8080 and 3128 POP3 traffic using TCP port 110 SMTP traffic using TCP port 25 See Section 20.1 on page 329 if you need to use the anti-virus scanner for FTP, HTTP, POP3 or SMTP traffic on custom ports.

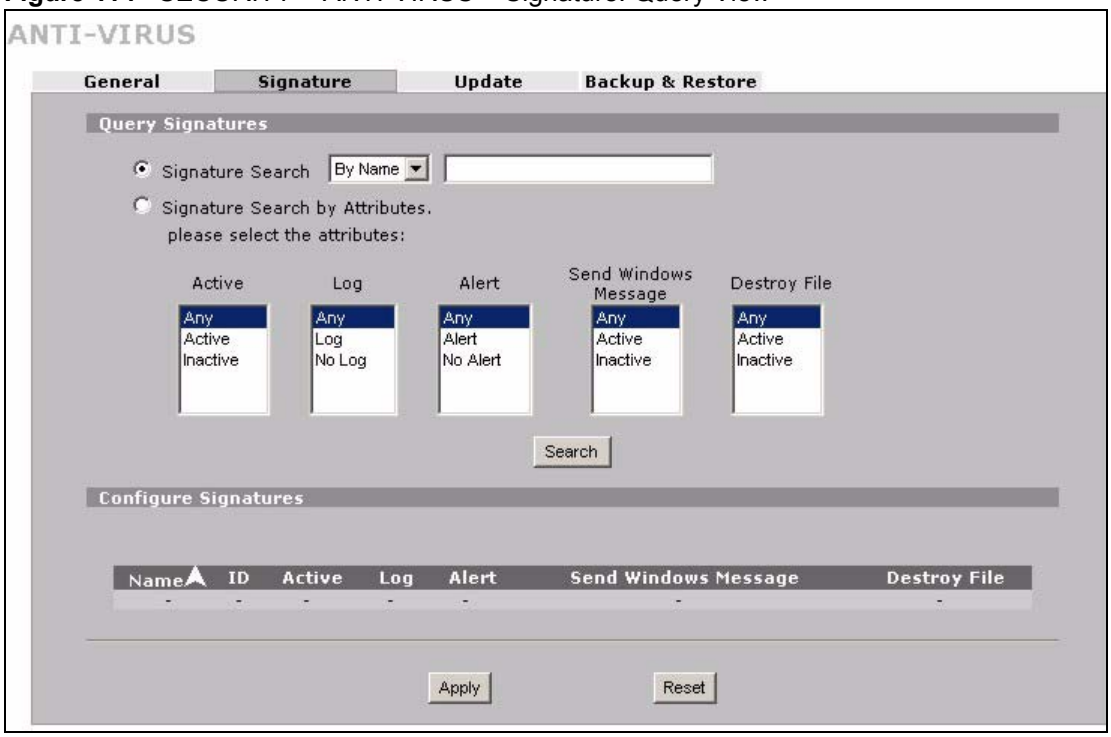
Table 56 SECURITY > ANTI-VIRUS > General (continued)

LABEL	DESCRIPTION
Active	Select **Active** to enable the anti-virus scanner for the selected service.
From, To	Select the directions of travel of packets that you want to check. Select or clear a row or column's first check box (with the interface label) to select or clear the interface's whole row or column. For example, **From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the ZyWALL or the ZyWALL itself. The ZyWALL does not check packets traveling from a LAN computer to another LAN computer on the same subnet. **From VPN** means traffic that came into the ZyWALL through the VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN or terminating at the ZyWALL's LAN interface. The ZyWALL checks the traffic after decrypting it. **To VPN** is traffic that comes in through the selected "from" interface and goes out through the VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through the VPN tunnel. The ZyWALL checks the traffic before encrypting it. **From VPN To VPN** means traffic that comes in through the VPN tunnel and terminates at the ZyWALL. This is the case if you allow someone to use a service (like Telnet or HTTP) through the VPN tunnel to manage the ZyWALL. The ZyWALL checks the traffic after decrypting it (before encrypting it again). Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnel. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic).
Protected Interface	Select the interface(s) where you want the ZyWALL to scan files for viruses.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to start configuring this screen again.

12.4 Signature Searching

Click **SECURITY > ANTI-VIRUS > Signature** to display this screen. Use this screen to locate signatures and manage how the ZyWALL uses them.

Figure 114 SECURITY > ANTI-VIRUS > Signature: Query View



The following table describes the labels in this screen.

Table 57 SECURITY > ANTI-VIRUS > Signature: Query View

LABEL	DESCRIPTION
Query Signatures	Select the criteria on which to perform the search.
Signature Search	Select this radio button if you would like to search the signatures by name or ID. Select this check box to only select the signatures you created or imported in the **Custom Signature** screen by name or ID. Select **By Name** from the drop down list box and type the name or part of the name of the signature(s) you want to find. Select **By ID** from the drop down list box and type the ID or part of the ID of the signature you want to find.
Signature Search by Attributes	Select this radio button if you would like to search the signatures by the general attributes listed next.
Active	Use this field to search for active (enabled) and/or inactive (disabled) signatures here.
Log	Search for signatures by log option here (whether or not the ZyWALL is set to log packets that match the signature).
Alert	Search for signatures by whether or not the ZyWALL is set to generate an alert mail when packets match the signature).
Send Windows Message	Search for signatures by whether or not the ZyWALL is set to send a message alert to files' intended user(s) using Microsoft Windows computer connected to the protected interface.
Destroy File	Search for signatures by whether or not the ZyWALL is set to erase the infected portion of the file before sending it.
Search	Click this button to begin the search. The results display in the table at the bottom of the screen. Results may be spread over several pages depending on how broad the search criteria selected were. The tighter the criteria selected, the fewer the (relevant) signatures returned.

Table 57 SECURITY > ANTI-VIRUS > Signature: Query View (continued)

LABEL	DESCRIPTION
Configure Signatures	The signature search results display in a table showing the SID, Name, Severity, Attack Type, Platform, Service, Activation, Log, and Action criteria as selected in the search. Click the SID column header to sort search results by SID.
Go to Page	Navigate between the pages of signature search results.
Name	This is the name of the anti-virus signature. Click the **Name** column heading to sort your search results in ascending or descending order according to the rule name.
ID	This is the IDentification number of the anti-virus signature. Click the ID column header to sort your search results by ID.
Active	Select **Active** to enable the anti-virus scanner for the selected signature. Select or clear the check box in the column heading to select or clear the column's check boxes for all of the displayed anti-virus signatures.
Log	Select **Log** to create a log when packets match the signature. Select or clear the check box in the column heading to select or clear the column's check boxes for all of the displayed anti-virus signatures.
Alert	This field is applicable only when you select **Log**. Select **Alert** to create an alert when a virus is detected. Select or clear the check box in the column heading to select or clear the column's check boxes for all of the displayed anti-virus signatures.
Send Windows Message	Select this check box to set the ZyWALL to send a message alert to files' intended user(s) using Microsoft Windows computer connected to the protected interface. Select or clear the check box in the column heading to select or clear the column's check boxes for all of the displayed anti-virus signatures.
Destroy File	Select this check box to set the ZyWALL to erase the infected portion of the file before sending it. Once destroyed, you may not be able to open the file. Select or clear the check box in the column heading to select or clear the column's check boxes for all of the displayed anti-virus signatures.
Apply	Click **Apply** to save your settings to the ZyWALL.
Reset	Click **Reset** to return to discard any unsaved changes that you have made in this screen and return to the previously saved settings.

12.4.1 Signature Search Example

This example shows a search for signatures that are enabled, set to generate logs and alerts, send Windows messages and destroy the infected portion of the file.

Figure 115 Query Example Search Criteria

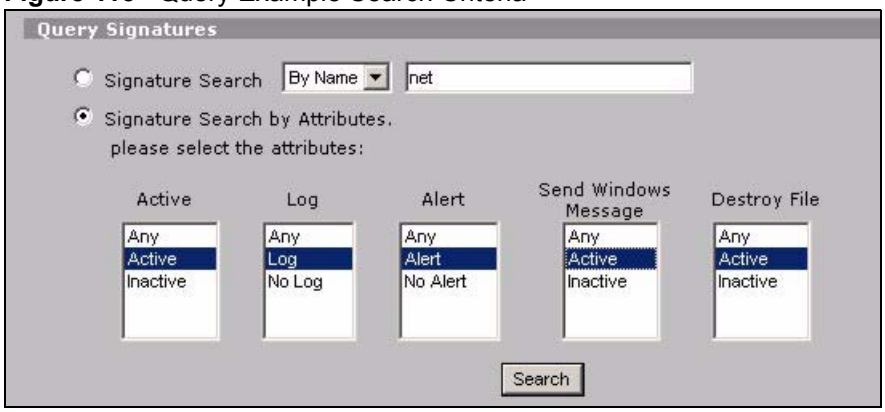
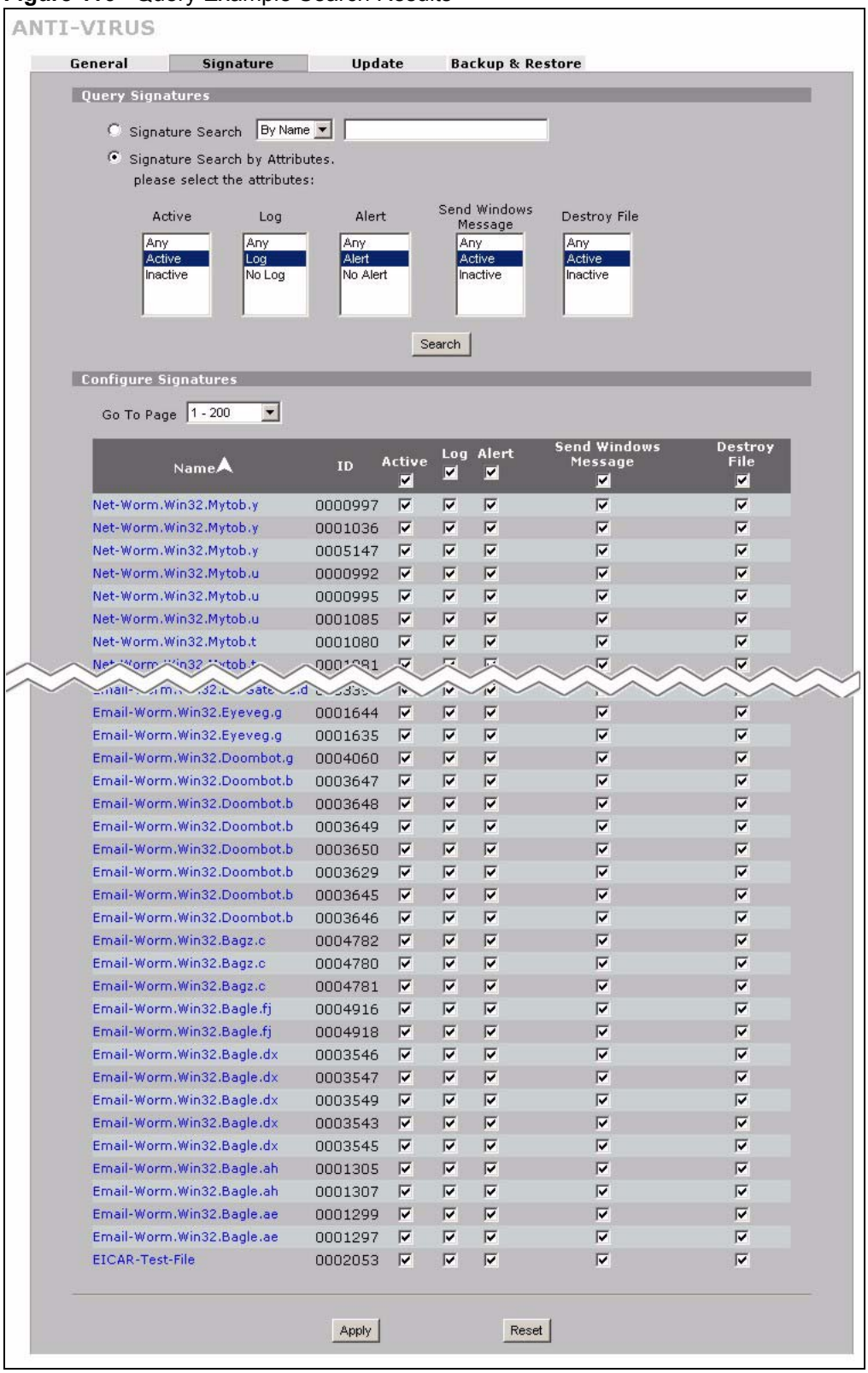


Figure 116 Query Example Search Results



12.5 Signature Update

The ZyWALL comes with built-in signatures created by the ZyXEL Security Response Team (ZSRT). These are regularly updated as new intrusions evolve. Use the **Update** screen to immediately download or schedule new signature downloads.

You should have already registered the ZyWALL at myZyXEL.com (http://www.myzyxel.com/myzyxel/) and also have either activated the trial license or standard license (iCard). If your license has expired, you will have to renew it before updates are allowed.

12.5.1 mySecurityZone

mySecurityZone is a web portal that provides all security-related information such as intrusion and anti-virus information for ZyXEL security products.

You should have already registered your ZyWALL on myZyXEL.com at:

http://www.myzyxel.com/myzyxel/.

You can use your myZyXEL.com username and password to log into mySecurityZone.

12.5.2 Configuring Anti-virus Update

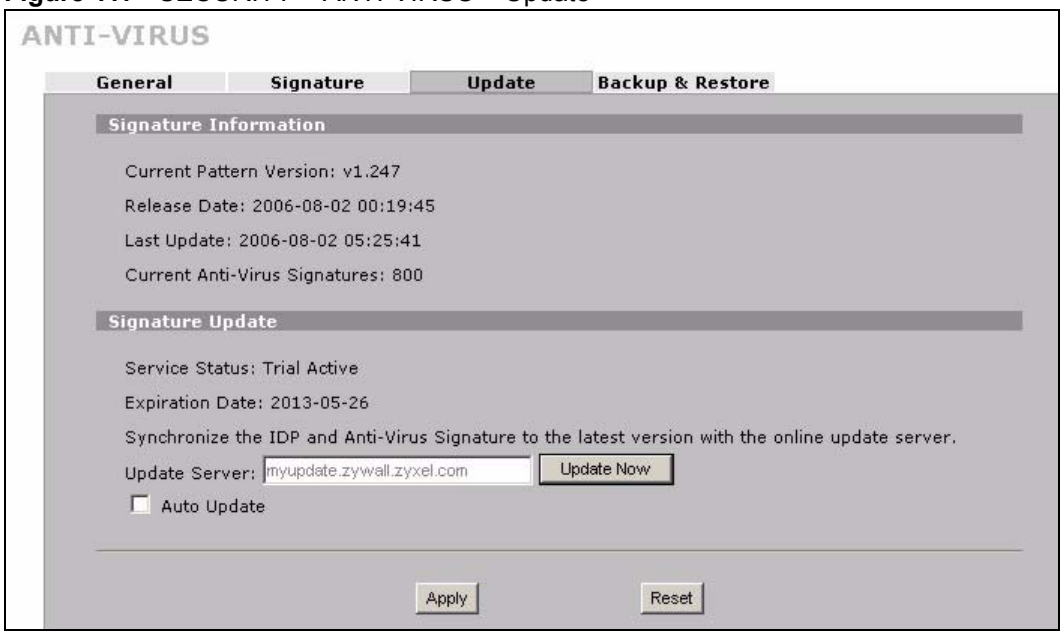
When scheduling signature updates, you should choose a day and time when your network is least busy so as to minimize disruption to your network. Your custom signature configurations are not over-written when you download new signatures.

IDP signatures (see the chapters on IDP) are included with file-based anti-virus signatures. When you download new signatures using the IDP **Update** screen, anti-virus signatures are also downloaded. The version number changes both in the IDP **Update** screen and this screen. Both screens also share the same **Auto-Update** schedule. Changes made to the schedule in one screen are reflected in the other.

The ZyWALL does not have to reboot when you upload new signatures.

Click **SECURITY** > **ANTI-VIRUS** > **Update**.

Figure 117 SECURITY > ANTI-VIRUS > Update



The following table describes the labels in this screen.

Table 58 SECURITY > ANTI-VIRUS > Update

LABEL	DESCRIPTION
Signature Information	
Current Pattern Version	This field displays the signatures version number currently used by the ZyWALL. This number is defined by the ZyXEL Security Response Team (ZSRT) who maintain and update them. This number increments as new signatures are added, so you should refer to this number regularly. Go to https://mysecurity.zyxel.com/mysecurity/ to see what the latest version number is. You can also subscribe to signature update e-mail notifications.
Release Date	This field displays the time (hour, minutes second) and date (month, date, year) that the above signature set was created.
Last Update	This field displays the last date and time you downloaded new signatures to the ZyWALL. It displays **N/A** if you have not downloaded any new signatures yet.
Current Anti-Virus Signatures	This field displays the number of Anti-Virus-related signatures.
Signature Update	
Service Status	This field displays **License Inactive** if you have not yet activated your trial or iCard license at myZyXEL.com. It displays **License Inactive** and an expiration date if your trial or iCard license has expired (the expiration date is the date it expired). It displays **Trial Active** and an expiration date when you have activated your trial license. It displays **License Active** and an expiration date when you have activated your iCard license (the expiration date is the date it will expire).
Update Server	This is the URL of the signature server from which you download signatures.
Update Now	Click this button to begin downloading signatures from the **Update Server** immediately.

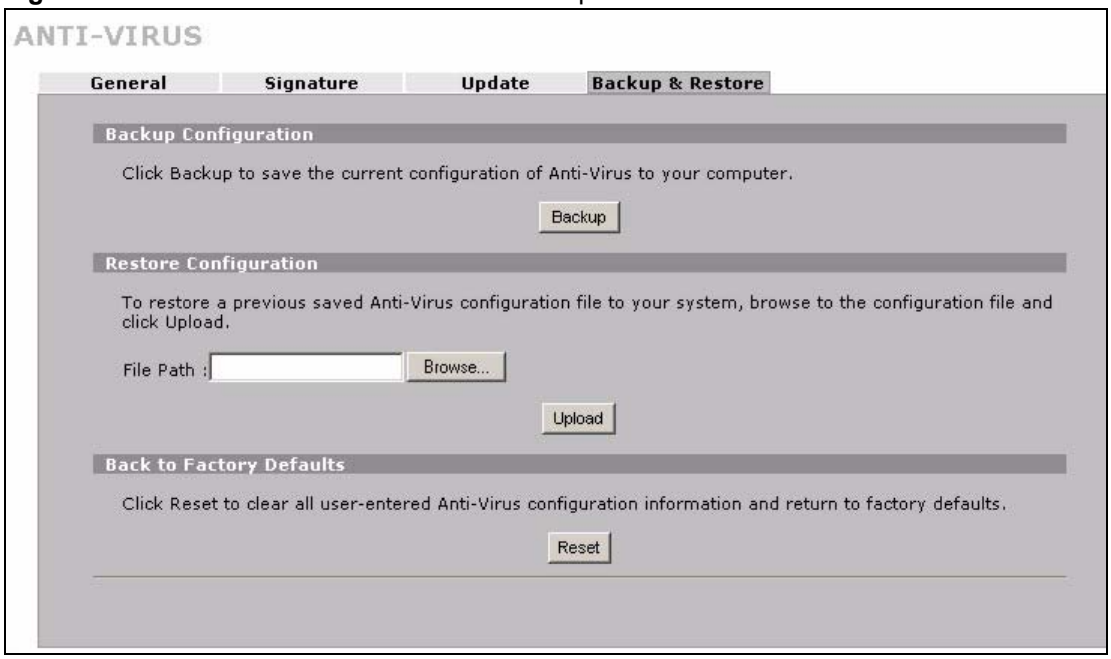
Table 58 SECURITY > ANTI-VIRUS > Update (continued)

LABEL	DESCRIPTION
Auto Update	Select the check box to configure a schedule for automatic signature updates. The **Hourly**, **Daily** and **Weekly** fields display when the check box is selected. The ZyWALL then automatically downloads signatures from the **Update Server** regularly at the time and/or day you specify.
Hourly	Select this option to have the ZyWALL check the update server for new signatures every hour. This may be advisable when new viruses are currently spreading throughout the Internet.
Daily	Select this option to have the ZyWALL check the update server for new signatures every day at the hour you select from the list box. The ZyWALL uses a 24-hour clock. For example, choose 15 from the **O'clock** list box to have the ZyWALL check the update server for new signatures at 3 PM every day.
Weekly	Select this option to have the ZyWALL check the update server for new signatures once a week on the day and hour you select from the list boxes. The ZyWALL uses a 24-hour clock, so for example, choose **Wednesday** and **15** from the respective list boxes to have the ZyWALL check the update server for new signatures at 3PM every Wednesday.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to close this screen without saving any changes.

12.6 Backup and Restore

Click **ANTI-VIRUS** > **Backup & Restore**. The screen displays as shown next. You can change the pre-defined **Active**, **Log**, **Alert**, **Send Windows Message** and/or **Destroy File** settings of individual signatures.

Figure 118 SECURITY > ANTI-VIRUS > Backup and Restore


ANTI-VIRUS
General
Signature
Update
Backup & Restore
Backup Configuration
Click Backup to save the current configuration of Anti-Virus to your computer.
Backup
Restore Configuration
To restore a previous saved Anti-Virus configuration file to your system, browse to the configuration file and click Upload.
File Path :
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered Anti-Virus configuration information and return to factory defaults.
Reset

Use the **Backup & Restore** screen to:

- Back up anti-virus signatures with your custom configured settings to a computer. Click **Backup** and then choose a location and filename for the anti-virus configuration set.
- Restore previously saved anti-virus signatures (with your custom configured settings). Click **Restore** and choose the path and location where the previously saved file resides on your computer.
- Revert to the original ZSRT-defined signature **Active**, **Log**, **Alert**, **Send Windows Message** and/or **Destroy File** settings. Click **Reset**.

13

IPSec VPN

This chapter explains how to set up and maintain IPSec VPNs in the ZyWALL. First, it provides an overview of IPSec VPNs. Then, it introduces each screen for IPSec VPN in the ZyWALL.

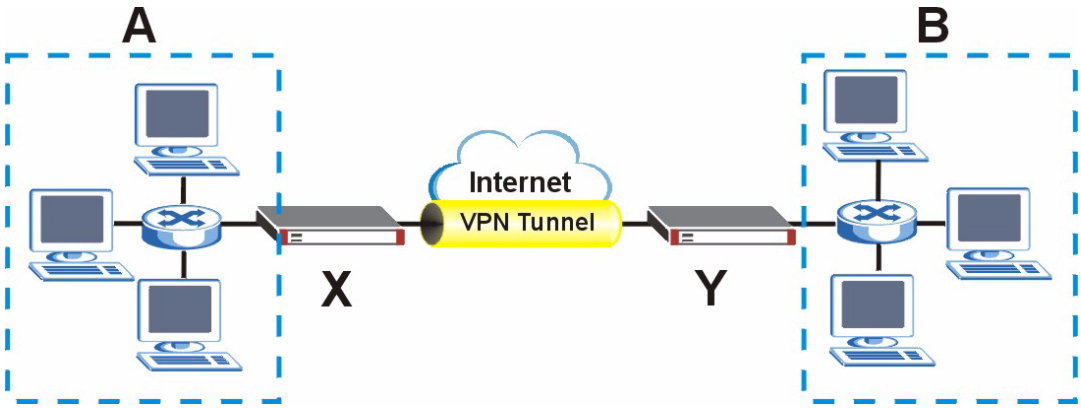
13.1 IPSec VPN Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The following figure provides one perspective of a VPN tunnel.

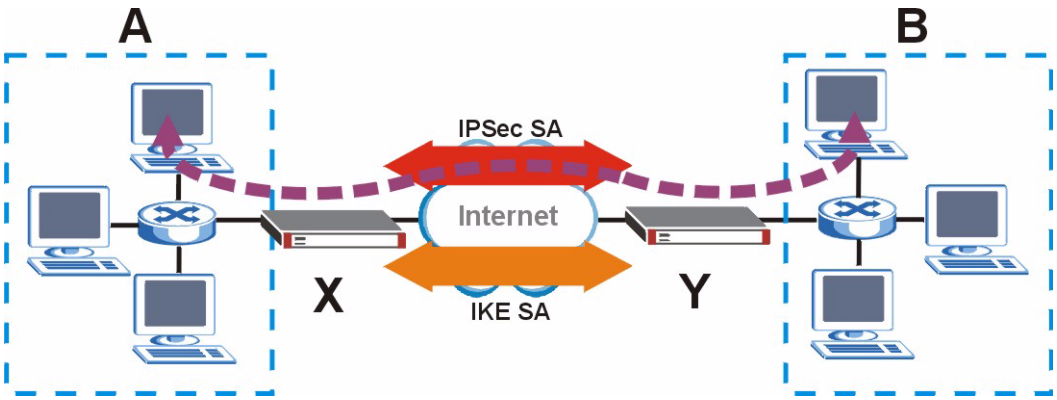
Figure 119 VPN: Example



The VPN tunnel connects the ZyWALL (**X**) and the remote IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyWALL and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyWALL and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the ZyWALL and remote IPSec router can send data between computers on the local network and remote network. The following figure illustrates this.

Figure 120 VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is established securely using the IKE SA that routers **X** and **Y** established first.

The rest of this section discusses IKE SA and IPSec SA in more detail.

13.1.1 IKE SA Overview

The IKE SA provides a secure connection between the ZyWALL and remote IPSec router.

It takes several steps to establish an IKE SA. The negotiation mode determines the number of steps to use. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Both routers must use the same negotiation mode.

These modes are discussed in more detail in Section 13.3.1.4 on page 211. Main mode is used in various examples in the rest of this section.

13.1.1.1 IP Addresses of the ZyWALL and Remote IPSec Router

In the ZyWALL, you have to specify the IP addresses of the ZyWALL and the remote IPSec router to establish an IKE SA.

You can usually provide a static IP address or a domain name for the ZyWALL. Sometimes, your ZyWALL might also offer another alternative, such as using the IP address of a port or interface.

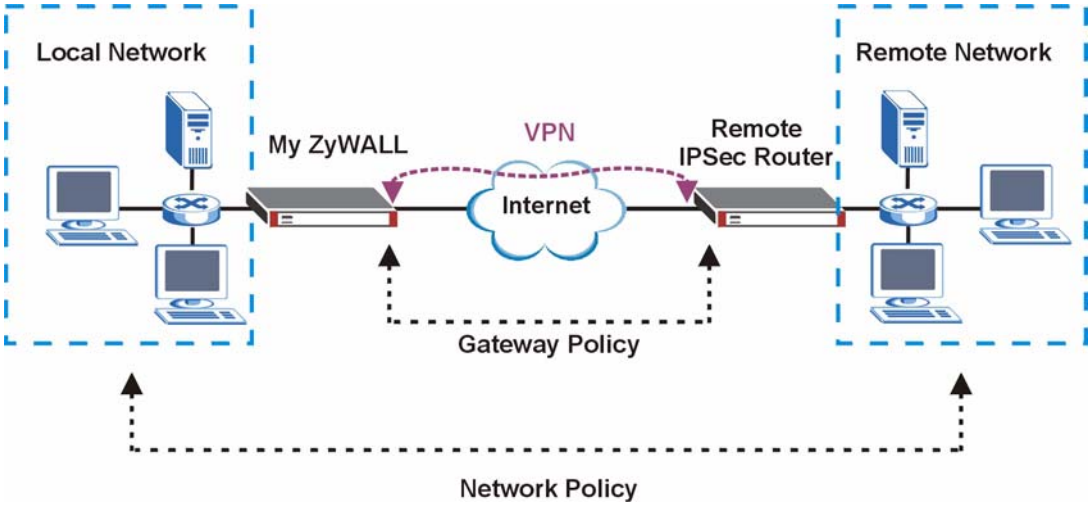
You can usually provide a static IP address or a domain name for the remote IPSec router as well. Sometimes, you might not know the IP address of the remote IPSec router (for example, telecommuters). In this case, you can still set up the IKE SA, but only the remote IPSec router can initiate an IKE SA.

13.2 VPN Rules (IKE)

A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network.

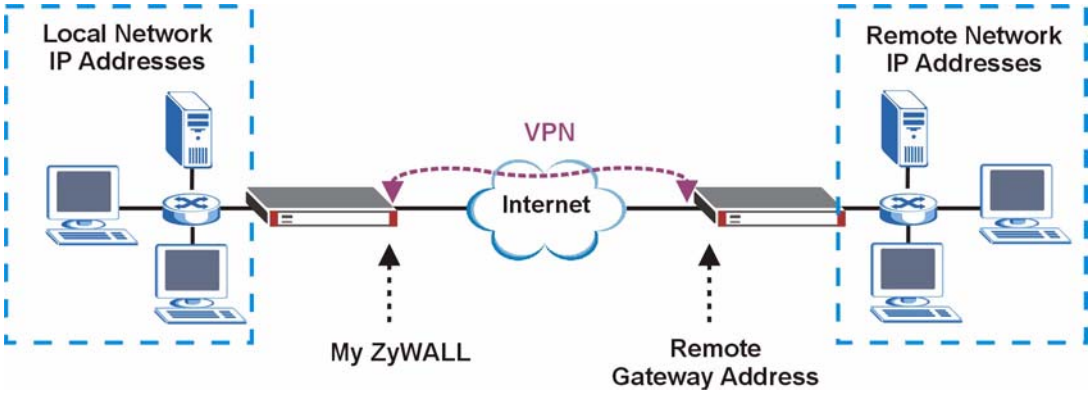
- A gateway policy contains the IKE SA settings. It identifies the IPSec routers at either end of a VPN tunnel.
- A network policy contains the IPSec SA settings. It specifies which devices (behind the IPSec routers) can use the VPN tunnel.

Figure 121 Gateway and Network Policies



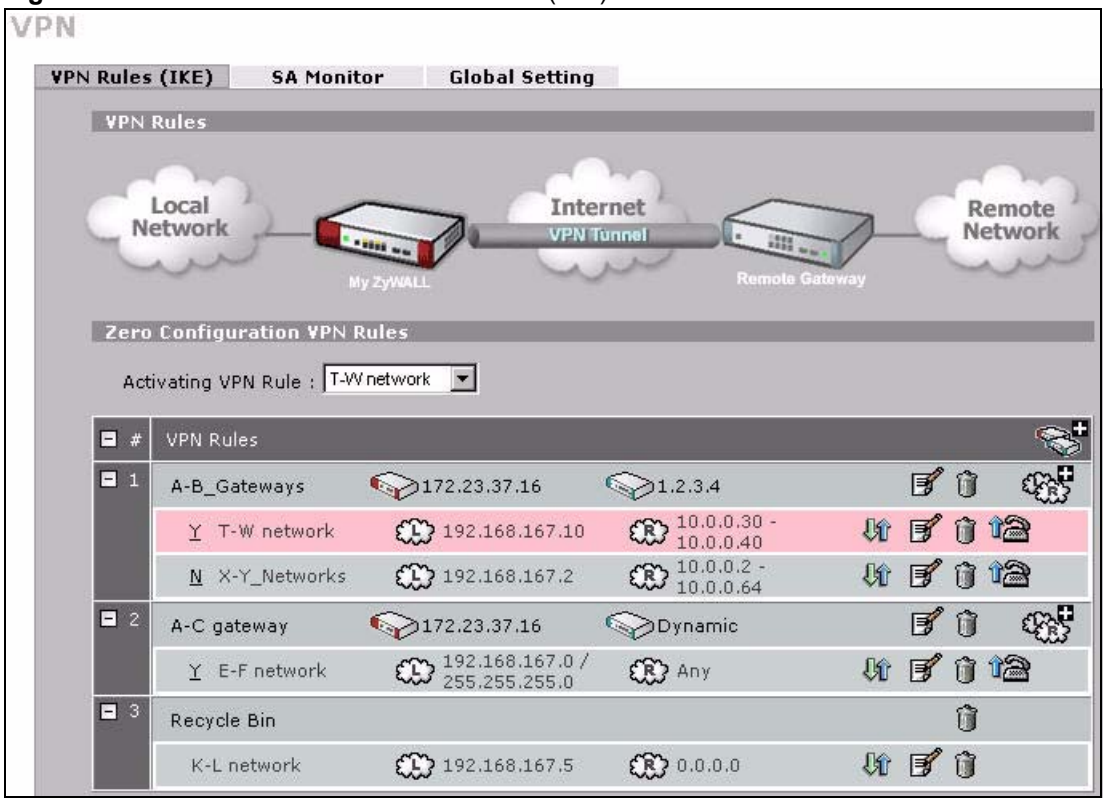
This figure helps explain the main fields in the VPN setup.

Figure 122 IPSec Fields Summary



Click **SECURITY > VPN** to display the **VPN Rules (IKE)** screen. Use this screen to manage the ZyWALL's list of VPN rules (tunnels) that use IKE SAs.

Figure 123 SECURITY > VPN > VPN Rules (IKE)



The following table describes the labels in this screen.

Table 59 SECURITY > VPN > VPN Rules (IKE)

LABEL	DESCRIPTION
Activating VPN Rule	Select the VPN network policy that you want the ZyWALL to use while in zero configuration mode. This stops unauthorized use of the other network policies. The row for the network policy you select displays in pink. N/A means that none of the VPN rules can be used. You cannot select a network policy that is in the recycle bin. This field changes to N/A if you delete the selected policy or move it to the recycle bin.
+/-	In the heading row, click + to expand or - to collapse the VPN rule network policies.
VPN Rules	These VPN rules define the settings for creating VPN tunnels for secure connection to other computers or networks.
	Click this icon to add a VPN gateway policy (or IPSec rule).
#	This is your VPN rule number. Click + to expand or - to collapse the VPN rule's network policies.
Gateway Policies	The first row of each VPN rule represents the gateway policy. The gateway policy identifies the IPSec routers at either end of a VPN tunnel (**My ZyWALL** and **Remote Gateway**) and specifies the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA (click the edit icon to display the other settings).

Table 59 SECURITY > VPN > VPN Rules (IKE) (continued)

LABEL	DESCRIPTION
My ZyWALL	This represents your ZyWALL. The WAN IP address, domain name or dynamic domain name of your ZyWALL displays in router mode. The ZyWALL's IP address displays in bridge mode.
Remote Gateway	This represents the remote secure gateway. The IP address, domain name or dynamic domain name of the remote IPSec router displays if you specify it, otherwise **Dynamic** displays.
	Click this icon to add a VPN network policy.
Y/N	This field displays whether a network policy is turned on (**Y**) or not (**N**). Click the letter to change it to the other state (click **Y** to change it to **N** or **N** to change it to **Y**).
Network Policies	The subsequent rows in a VPN rule are network policies. A network policy identifies the devices behind the IPSec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.
Local Network	This is the network behind the ZyWALL. A network policy specifies which devices (behind the IPSec routers) can use the VPN tunnel.
Remote Network	This is the remote network behind the remote IPsec router.
	Click this icon to display a screen in which you can associate a network policy to a gateway policy or move it to the recycle bin.
	Click this icon to display a screen in which you can change the settings of a gateway or network policy.
	Click this icon to delete a gateway or network policy. When you delete a gateway, the ZyWALL automatically moves the associated network policy(ies) to the recycle bin. When you delete a network policy, it is just deleted.
	Click this icon to establish a VPN connection to a remote network.
	Click this icon to drop a VPN connection to a remote network.
Recycle Bin	The recycle bin appears when you have any network policies that are not associated to a gateway policy. When you delete a gateway, the ZyWALL automatically moves the associated network policy(ies) to the recycle bin. You can also manually move a network policy that you do not need (but may want to use again later) to the recycle bin. Click the network policy's move or edit icon and set it's Gateway Policy to Recycle Bin.

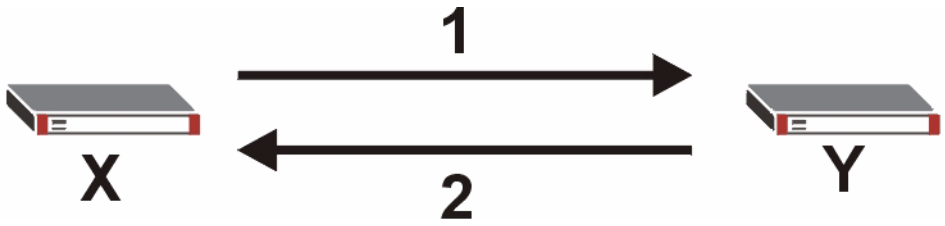
13.3 IKE SA Setup

This section provides more details about IKE SAs.

13.3.1 IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the ZyWALL and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated below.

Figure 124 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal



The ZyWALL sends one or more proposals to the remote IPSec router. (In some devices, you can set up only one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the ZyWALL wants to use in the IKE SA. The remote IPSec router selects an acceptable proposal and sends the accepted proposal back to the ZyWALL. If the remote IPSec router rejects all of the proposals (for example, if the VPN tunnel is not configured correctly), the ZyWALL and remote IPSec router cannot establish an IKE SA.

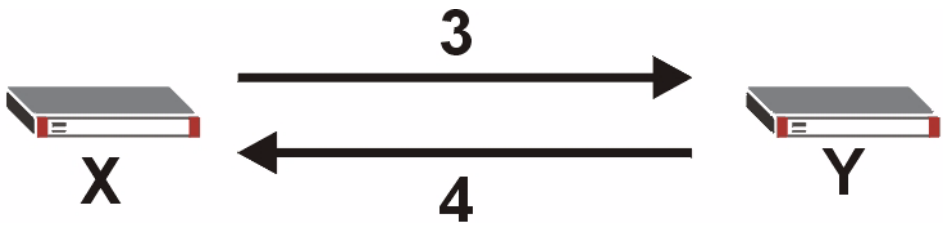
Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

See the field descriptions for information about specific encryption algorithms, authentication algorithms, and DH key groups. See Section 13.3.1.1 on page 208 for more information about DH key groups.

13.3.1.1 Diffie-Hellman (DH) Key Exchange

The ZyWALL and the remote IPSec router use a DH key exchange to establish a shared secret, which is used to generate encryption keys for IKE SA and IPSec SA. In main mode, the DH key exchange is done in steps 3 and 4, as illustrated below.

Figure 125 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



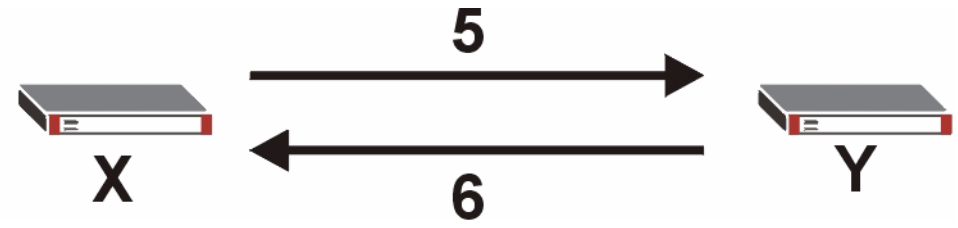
The DH key exchange is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption keys, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 encryption keys take longer to encrypt and decrypt.

13.3.1.2 Authentication

Before the ZyWALL and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the ZyWALL and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. Their identities are encrypted using the encryption algorithm and encryption key the ZyWALL and remote IPSec router selected in previous steps.

Figure 126 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication



The ZyWALL and remote IPSec router use a pre-shared key in the authentication process, though it is not actually transmitted or exchanged.

The ZyWALL and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and ID content. The ID type can be IP address, domain name, or e-mail address, and the ID content is a specific IP address, domain name, or e-mail address. The ID content is only used for identification; the IP address, domain name, or e-mail address that you enter does not have to actually exist.

The ZyWALL and the remote IPSec router each has its own identity, so each one must store two sets of information, one for itself and one for the other router. Local ID type and ID content refers to the ID type and ID content that applies to the router itself, and peer ID type and ID content refers to the ID type and ID content that applies to the other router in the IKE SA.

The ZyWALL's local and peer ID type and ID content must match the remote IPSec router's peer and local ID type and ID content, respectively.

In the following example, the ID type and content match so the ZyWALL and the remote IPSec router authenticate each other successfully.

Table 60 VPN Example: Matching ID Type and Content

ZYWALL	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

In the following example, the ID type and content do not match so the authentication fails and the ZyWALL and the remote IPSec router cannot establish an IKE SA.

Table 61 VPN Example: Mismatching ID Type and Content

ZYWALL	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.15	Peer ID content: tom@yourcompany.com

It is also possible to configure the ZyWALL to ignore the identity of the remote IPSec router. In this case, you usually set the peer ID type to **Any**. This is not as secure as other peer ID types, however.

13.3.1.2.1 Certificates

It is also possible for the ZyWALL and remote IPSec router to authenticate each other with certificates. In this case, the authentication process is different.

- Instead of using the pre-shared key, the ZyWALL and remote IPSec router check each other's certificates.
- The local ID type and ID content come from the certificate. On the ZyWALL, you simply select which certificate to use.
- If you set the peer ID type to **Any**, the ZyWALL authenticates the remote IPSec router using the trusted certificates and trusted CAs you have set up. Alternatively, if you want to use a specific certificate to authenticate the remote IPSec router, you can use the information in the certificate to specify the peer ID type and ID content.

You must set up the certificates for the ZyWALL and remote IPSec router before you can use certificates in IKE SA. See Chapter 14 on page 243 for more information about certificates.

13.3.1.3 Extended Authentication

Extended authentication is often used when multiple IPSec routers use the same VPN tunnel to connect to a single IPSec router. For example, this might be used with telecommuters. Extended authentication occurs right after the authentication described in Section 13.3.1.2 on page 208.

In extended authentication, one of the routers (the ZyWALL or the remote IPSec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the ZyWALL to provide a user name and password to the remote IPSec router, or you can set up the ZyWALL to check a user name and password that is provided by the remote IPSec router.

13.3.1.4 Negotiation Mode

There are two negotiation modes: main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1-2: The ZyWALL sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the ZyWALL.

Steps 3-4: The ZyWALL and the remote IPSec router participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

Steps 5-6: Finally, the ZyWALL and the remote IPSec router generate an encryption key from the shared secret, encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA.

Step 1: The ZyWALL sends its proposals to the remote IPSec router. It also starts the Diffie-Hellman key exchange and sends its (unencrypted) identity to the remote IPSec router for authentication.

Step 2: The remote IPSec router selects an acceptable proposal and sends it back to the ZyWALL. It also finishes the Diffie-Hellman key exchange, authenticates the ZyWALL, and sends its (unencrypted) identity to the ZyWALL for authentication.

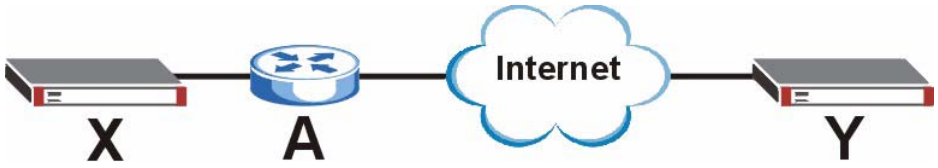
Step 3: The ZyWALL authenticates the remote IPSec router and confirms that the IKE SA is established.

Aggressive mode does not provide as much security as main mode because the identity of the ZyWALL and the identity of the remote IPSec router are not encrypted. It is usually used when the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication (for example, telecommuters).

13.3.1.5 VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

Figure 127 VPN/NAT Example



If router **A** does NAT, it might change the IP addresses, port numbers, or both. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router **A** now have an IPSec pass-through feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the active protocol is ESP. (See Section 13.6.3 on page 223 for more information about active protocols.)

If router A does not have an IPSec pass-through or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the ZyWALL and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged. (See the field description for detailed information about the extra header.)

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the ZyWALL and remote IPSec router support.

13.4 Additional IPSec VPN Topics

This section discusses other IPSec VPN topics that apply to either IKE SAs or IPSec SAs or both. Relationships between the topics are also highlighted.

13.4.1 Dynamic IPSec Rule

Create a dynamic rule by setting the **Primary Remote Address** to '0.0.0.0'. A single dynamic rule can support multiple simultaneous incoming IPSec connections.

All users of a dynamic rule have the same pre-shared key. You may need to change the pre-shared key if one of the users leaves. See the support notes at http://www.zyxel.com for configuration examples for software VPN clients.

13.4.2 Full Feature NAT Mode

With **Full Feature** NAT mode, you must map the intended VPN rule's local policy addresses as the Inside Local Address (ILA) to a public IP address assigned by the ISP (an Inside Global Address or IGA) before you can configure the VPN rule. For example, you could create a One-to-One address mapping rule that maps the VPN rule's local policy addresses as the ILA to the VPN rule's my IP address as the IGA.

You may have to specify the public IP address in the **My ZyWALL** field of the local IPSec rule. If you have not configured the address mapping properly, a "SPD doesn't match configuration of NAT" message displays when you try to save the IPSec rule.

13.4.3 SA Life Time

SAs have a lifetime that specifies how long the SA lasts until it times out. When an SA times out, the ZyWALL automatically renegotiates the SA in the following situations:

- There is traffic when the SA life time expires
- The IPSec SA is configured on the ZyWALL as nailed up (see below)

Otherwise, the ZyWALL must re-negotiate the SA the next time someone wants to send traffic.

If the IKE SA times out while an IPSec SA is connected, the IPSec SA stays connected.

An IPSec SA can be set to **nailed up**. Normally, the ZyWALL drops the IPSec SA when the life time expires or after two minutes of outbound traffic with no inbound traffic. If you set the IPSec SA to nailed up, the ZyWALL automatically renegotiates the IPSec SA when the SA life time expires, and it does not drop the IPSec SA if there is no inbound traffic.

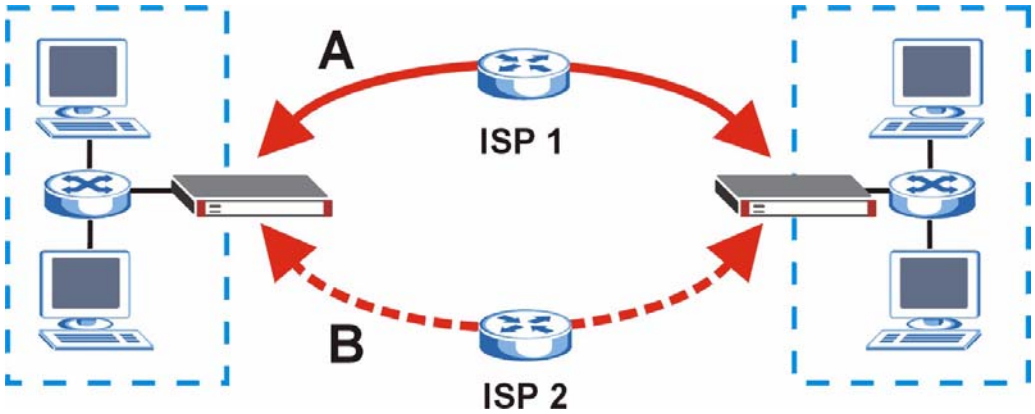
The SA life time and nailed up settings only apply if the rule identifies the remote IPSec router by a static IP address or a domain name. If the **Primary Remote Address** field is set to **0.0.0.0**, the ZyWALL cannot initiate the tunnel (and cannot renegotiate the SA).

13.4.4 IPSec High Availability

IPSec high availability (also known as VPN high availability) allows you to use a redundant (backup) VPN connection to another WAN interface on the remote IPSec router if the primary (regular) VPN connection goes down.

In the following figure, if the primary VPN tunnel (A) goes down, the ZyWALL uses the redundant VPN tunnel (B).

Figure 128 IPSec High Availability



When setting up a IPSec high availability VPN tunnel, the remote IPSec router:

- Must have multiple WAN connections.
- Only needs the configure one corresponding IPSec rule.
- Should only have IPSec high availability settings in its corresponding IPSec rule if your ZyWALL has multiple WAN connections.
- Should ideally identify itself by a domain name or dynamic domain name (it must otherwise have **My Address** set to 0.0.0.0).

- Should use a WAN connectivity check to this ZyWALL's WAN IP address.

If the remote IPSec router is not a ZyWALL, you may also want to avoid setting the IPSec rule to nailed up.

13.4.5 Encryption and Authentication Algorithms

In most ZyWALLs, you can select one of the following encryption algorithms for each proposal. The encryption algorithms are listed here in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.
- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.

Use the commands to have the AES encryption apply 192-bit or 256-bit keys to 128-bit blocks of data.

You can select one of the following authentication algorithms for each proposal. The algorithms are listed here in order from weakest to strongest.

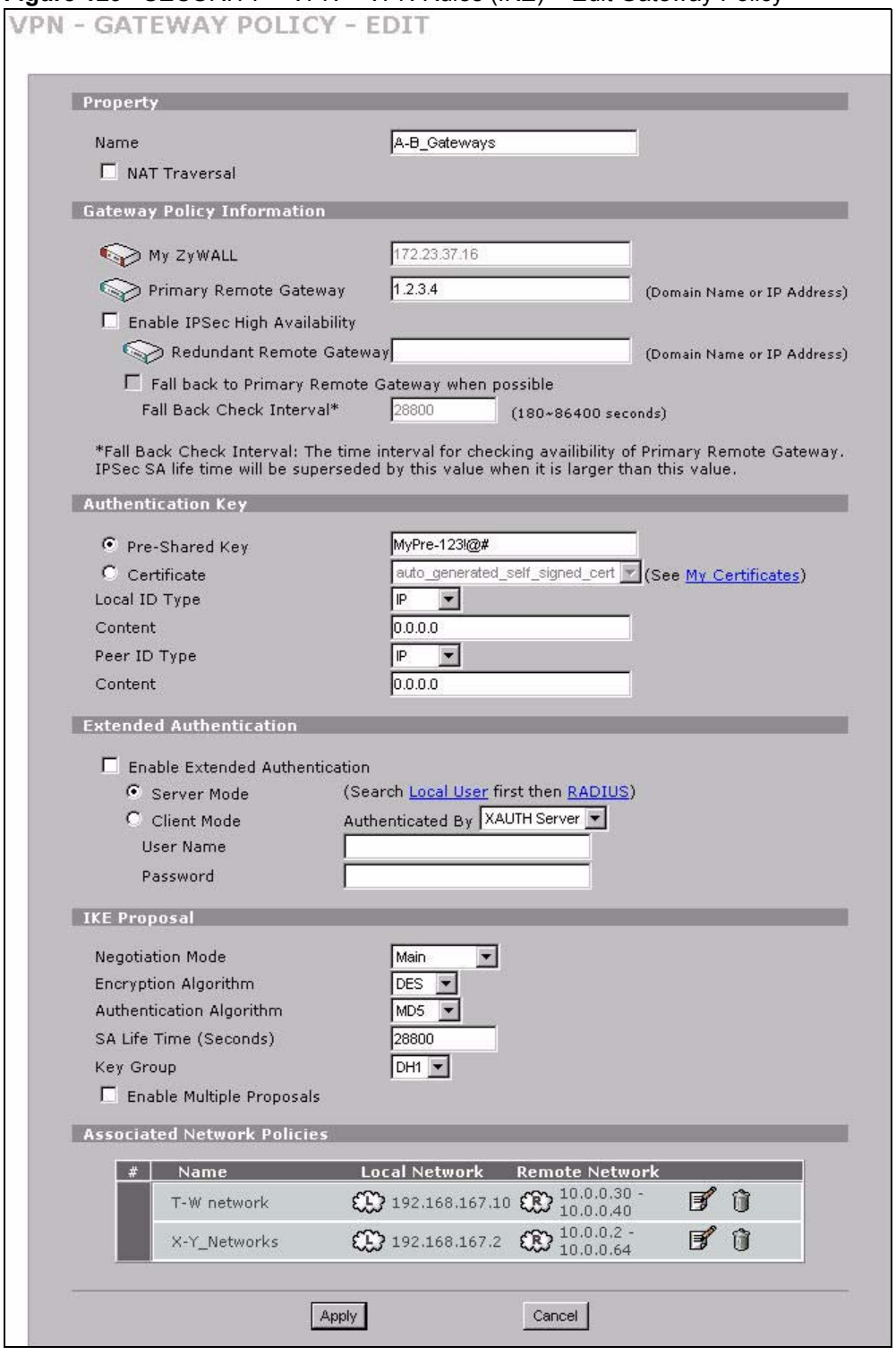
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

13.5 VPN Rules (IKE) Gateway Policy Edit

In the **VPN Rule (IKE)** screen, click the add gateway policy ( ) icon or the edit ( ) icon to display the **VPN-Gateway Policy -Edit** screen.

Use this screen to configure a VPN gateway policy. The gateway policy identifies the IPSec routers at either end of a VPN tunnel (**My ZyWALL** and **Remote Gateway**) and specifies the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA.

Figure 129 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy



The following table describes the labels in this screen.

Table 62 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy

LABEL	DESCRIPTION
Property	
Name	Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. Note: The remote IPSec router must also have NAT traversal enabled. See Section 13.3.1.5 on page 211 for more information. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP ports 500 and 4500 to the IPSec router behind the NAT router.
Gateway Policy Information	
My ZyWALL	When the ZyWALL is in router mode, this field identifies the WAN IP address or domain name of the ZyWALL. You can select **My Address** and enter the ZyWALL's static WAN IP address (if it has one) or leave the field set to 0.0.0.0. The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. Otherwise, you can select **My Domain Name** and choose one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the ZyWALL use that dynamic domain name's IP address. When the ZyWALL is in bridge mode, this field is read-only and displays the ZyWALL's IP address. The VPN tunnel has to be rebuilt if the **My ZyWALL** IP address changes after setup.
Primary Remote Gateway	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address. In order to have more than one active rule with the **Primary Remote Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Primary Remote Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Primary Remote Address** field set to **0.0.0.0**.
Enable IPSec High Availability	Turn on the high availability feature to use a redundant (backup) VPN connection to another WAN interface on the remote IPSec router if the primary (regular) VPN connection goes down. The remote IPSec router must have a second WAN connection in order for you to use this. To use this, you must identify both the primary and the redundant remote IPSec routers by WAN IP address or domain name (you cannot set either to **0.0.0.0**).
Redundant Remote Gateway	Type the WAN IP address or the domain name (up to 31 characters) of the backup IPSec router to use when the ZyWALL cannot not connect to the primary remote gateway.
Fall back to Primary Remote Gateway when possible	Select this to have the ZyWALL change back to using the primary remote gateway if the connection becomes available again.

Table 62 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

LABEL	DESCRIPTION
Fall Back Check Interval*	Set how often the ZyWALL should check the connection to the primary remote gateway while connected to the redundant remote gateway. Each gateway policy uses one or more network policies. If the fall back check interval is shorter than a network policy's SA life time, the fall back check interval is used as the check interval and network policy SA life time. If the fall back check interval is longer than a network policy's SA life time, the SA lifetime is used as the check interval and network policy SA life time.
Authentication Key	
Pre-Shared Key	Select the **Pre-Shared Key** radio button and type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.
Certificate	Select the **Certificate** radio button to identify the ZyWALL by a certificate. Use the drop-down list box to select the certificate to use for this VPN tunnel. You must have certificates already configured in the **My Certificates** screen. Click **My Certificates** to go to the **My Certificates** screen where you can view the ZyWALL's list of certificates.
Local ID Type	Select **IP** to identify this ZyWALL by its IP address. Select **DNS** to identify this ZyWALL by a domain name. Select **E-mail** to identify this ZyWALL by an e-mail address. You do not configure the local ID type and content when you set **Authentication Key** to **Certificate**. The ZyWALL takes them from the certificate you select.
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The ZyWALL automatically uses the IP address in the **My ZyWALL** field (refer to the **My** ZyWALL field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations. 1. When there is a NAT router between the two IPSec routers. 2. When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this ZyWALL in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.

Table 62 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

LABEL	DESCRIPTION
Peer ID Type	Select from the following when you set **Authentication Key** to **Pre-shared Key**. Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address. Select from the following when you set **Authentication Key** to **Certificate**. Select **IP** to identify the remote IPSec router by the IP address in the subject alternative name field of the certificate it uses for this VPN connection. Select **DNS** to identify the remote IPSec router by the domain name in the subject alternative name field of the certificate it uses for this VPN connection. Select **E-mail** to identify the remote IPSec router by the e-mail address in the subject alternative name field of the certificate it uses for this VPN connection. Select **Subject Name** to identify the remote IPSec router by the subject name of the certificate it uses for this VPN connection. Select **Any** to have the ZyWALL not check the remote IPSec router's ID.
Content	The configuration of the peer content depends on the peer ID type. Do the following when you set **Authentication Key** to **Pre-shared Key**. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyWALL will use the address in the **Primary Remote Address** field (refer to the **Primary Remote Address** field description). For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations: 1. When there is a NAT router between the two IPSec routers. 2. When you want the ZyWALL to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses. Do the following when you set **Authentication Key** to **Certificate**. 1. For **IP**, type the IP address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyWALL will use the address in the **Primary Remote Address** field (refer to the **Primary Remote Address** field description). 2. For **DNS** or **E-mail**, type the domain name or e-mail address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection. 3. For **Subject Name**, type the subject name of the certificate the remote IPSec router will use for this VPN connection. Use up to255 ASCII characters including spaces. 4. For **Any**, the peer **Content** field is not available. 5. Regardless of how you configure the **ID Type** and **Content** fields, two active IPSec SAs cannot have both the local and remote IP address ranges overlap between rules.
Extended Authentication	
Enable Extended Authentication	Select this check box to activate extended authentication.

Table 62 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

LABEL	DESCRIPTION
Server Mode	Select **Server Mode** to have this ZyWALL authenticate extended authentication clients that request this VPN connection. You must also configure the extended authentication clients' usernames and passwords in the authentication server's local user database or a RADIUS server (see Chapter 15 on page 271). Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of user names and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server. During authentication, if the ZyWALL (in server mode) does not find the extended authentication clients' user name in its internal user database and an external RADIUS server has been enabled, it attempts to authenticate the client through the RADIUS server.
Client Mode	Select **Client Mode** to have your ZyWALL use a username and password when initiating this VPN connection to the extended authentication server ZyWALL. Only a VPN extended authentication client can initiate this VPN connection.
Authenticated By	Select **XAUTH** to have the remote IPSec router authenticate user(s) that request this VPN connection. Note: You must also configure extended authentication on the remote IPsec router. Select **ZyWALL** to have your ZyWALL authenticate user(s) using a username and password when initiating this VPN connection. Select this option if the remote IPSec router is not configured to authenticate VPN user or does not have the extended authentication function. Select **None** to not authenticate user(s) that request this VPN connection.
User Name	Enter a user name for your ZyWALL to be authenticated by the VPN peer (in server mode). The user name can be up to 31 case-sensitive ASCII characters, but spaces are not allowed. You must enter a user name and password when you select client mode.
Password	Enter the corresponding password for the above user name. The password can be up to 31 case-sensitive ASCII characters, but spaces are not allowed.
IKE Proposal	
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES128** - a 128-bit key with the AES encryption algorithm **AES192** - a 192-bit key with the AES encryption algorithm **AES256** - a 256-bit key with the AES encryption algorithm The ZyWALL and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.

Table 62 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

LABEL	DESCRIPTION
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	Select which Diffie-Hellman key group (DH*x*) you want to use for encryption keys. Choices are: **DH1** - use a 768-bit random number **DH2** - use a 1024-bit random number **DH5** - use a 1536-bit random number The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Enable Multiple Proposals	Select this to allow the ZyWALL to use any of its phase 1 key groups and encryption and authentication algorithms when negotiating an IKE SA. When you enable multiple proposals, the ZyWALL allows the remote IPSec router to select which phase 1 key groups and encryption and authentication algorithms to use for the IKE SA, even if they are less secure than the ones you configure for the VPN rule. Clear this to have the ZyWALL use only the configured phase 1 key groups and encryption and authentication algorithms when negotiating an IKE SA.
Associated Network Policies	The following table shows the policy(ies) you configure for this rule. To add a VPN policy, click the add network policy ( ) icon in the **VPN Rules (IKE)** screen (see Figure 123 on page 206). Refer to Section 13.7 on page 225 for more information.
#	This field displays the policy index number.
Name	This field displays the policy name.
Local Network	This field displays one or a range of IP address(es) of the computer(s) behind the ZyWALL.
Remote Network	This field displays one or a range of IP address(es) of the remote network behind the remote IPsec router.
Edit	Click this icon to open the screen where you can configure the network policy.
Delete	Click this icon to remove the network policy.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

13.6 IPSec SA Overview

Once the ZyWALL and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

13.6.1 Local and Remote Networks

In an IPSec SA, the local network consists of devices connected to the ZyWALL and may be called the local policy. Similarly, the remote network consists of the devices connected to the remote IPSec router and may be called the remote policy.

You can configure a remote network as 0.0.0.0 (any) when:

- Forwarding all outgoing traffic to the remote gateway.
- The remote network's addresses are unknown or there are many remote networks using one VPN rule (see Section 13.14.1 on page 240 for an example of telecommuters sharing one VPN rule).

It is not recommended to set a VPN rule's local and remote network settings both to 0.0.0.0 (any).

In most cases you should use virtual address mapping (see Section 13.6.2 on page 221) to avoid overlapping local and remote network IP addresses. See Section 13.13 on page 236 for how the ZyWALL handles overlapping local and remote network IP addresses.

13.6.2 Virtual Address Mapping

Virtual address mapping (NAT over IPSec) changes the source IP addresses of packets from your local devices to virtual IP addresses before sending them through the VPN tunnel.

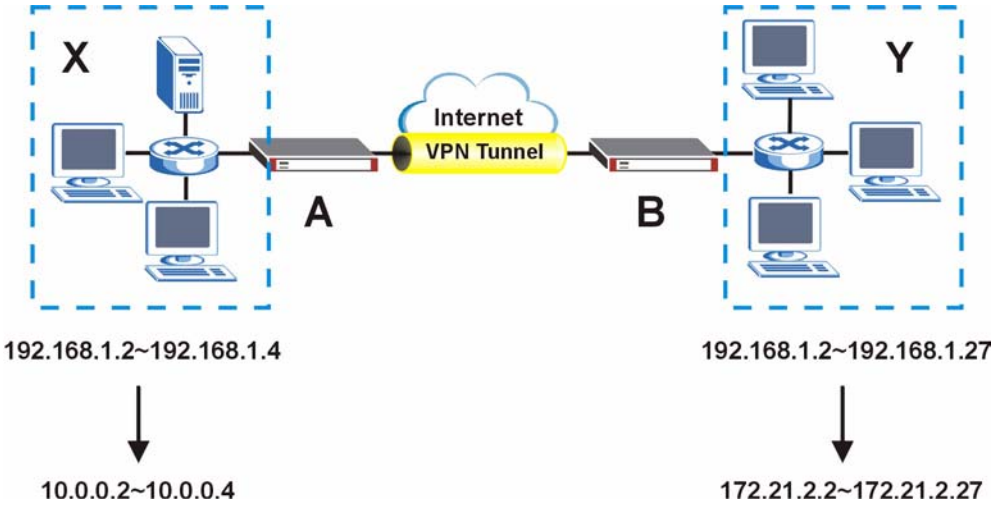
13.6.2.1 Avoiding Overlapping Local And Remote Network IP Addresses

If both IPSec routers support virtual address mapping, you can access devices on both networks, even if their IP addresses overlap. You map the ZyWALL's local network addresses to virtual IP addresses and map the remote IPSec router's local IP addresses to other (non-overlapping) virtual IP addresses.

The following diagram shows an example of using virtual address mapping to avoid overlapping local and remote IP addresses. You can set up virtual address mapping on both IPSec routers to allow computers on network **X** to access network **X** and network **Y** computers with the same IP address.

- You set ZyWALL **A** to change the source IP addresses of packets from local network **X** (192.168.1.2 to 192.168.1.4) to virtual IP addresses 10.0.0.2 to 10.0.0.4 before sending them through the VPN tunnel.
- You set ZyWALL **B** to change the source IP addresses of packets from the remote network **Y** (192.168.1.2 to 192.168.1.27) to virtual IP addresses 172.21.2.2 to 172.21.2.27 before sending them through the VPN tunnel.
- On ZyWALL **A**, you specify 172.21.2.2 to 172.21.2.27 as the remote network. On ZyWALL **B**, you specify 10.0.0.2 to 10.0.0.4 as the remote network.

Figure 130 Virtual Mapping of Local and Remote Network IP Addresses



Computers on network **X** use IP addresses 192.168.1.2 to 192.168.1.4 to access local network devices and IP addresses 172.21.2.2 to 172.21.2.27 to access the remote network devices.

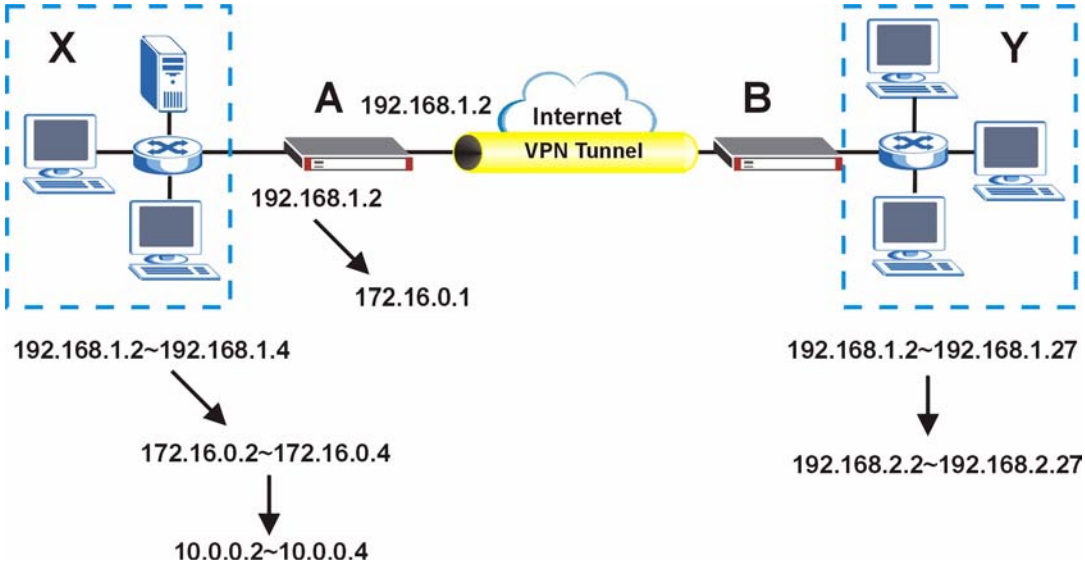
Computers on network **Y** use IP addresses 192.168.1.2 to 192.168.1.27 to access local network devices and IP addresses 10.0.0.2 to 10.0.0.4 to access the remote network devices.

13.6.2.2 Network Conflict Avoidance (Zero Configuration Mode)

Since your ZyWALL is portable, it may get (or you may need to configure) different WAN interface settings in different locations. In zero configuration mode, the ZyWALL automatically overwrites IPSec virtual address mapping settings and IPSec port forwarding rules (see Section 13.8 on page 230) in order to avoid network conflicts.

For example, ZyWALL **A** is assigned a WAN IP address of 192.168.1.2, which conflicts with its existing LAN IP address of 192.168.1.2. So in this example, ZyWALL **A** automatically changes its LAN IP address to 172.16.0.1 and the local network **X**'s (private) IP addresses to 172.16.0.2 to 172.16.0.4. With virtual mapping, ZyWALL **A** still translates the local network **X**'s (private) IP addresses to 10.0.0.2 to 10.0.0.4. So the VPN tunnel still works in the same way as if nothing had changed.

Figure 131 Virtual Mapping of Local and Remote Network IP Addresses



13.6.3 Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

The ZyWALL and remote IPSec router must use the same active protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

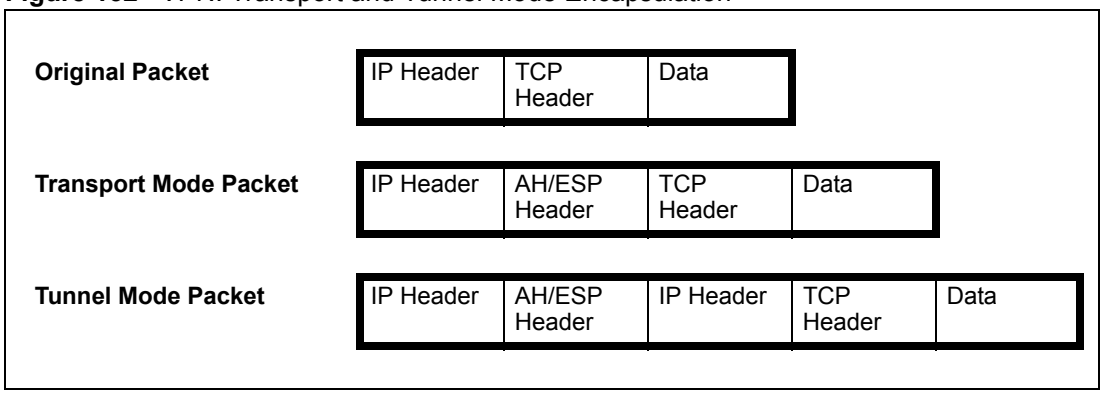
13.6.4 Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the ZyWALL and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

The ZyWALL and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

Figure 132 VPN: Transport and Tunnel Mode Encapsulation



In tunnel mode, the ZyWALL uses the active protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the ZyWALL or remote IPSec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the ZyWALL or remote IPSec router. The header for the active protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the active protocol. With AH, the ZyWALL includes part of the original IP header when it encapsulates the packet. With ESP, however, the ZyWALL does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

13.6.5 IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see Section 13.3.1 on page 207), except that you also have the choice whether or not the ZyWALL and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the ZyWALL and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

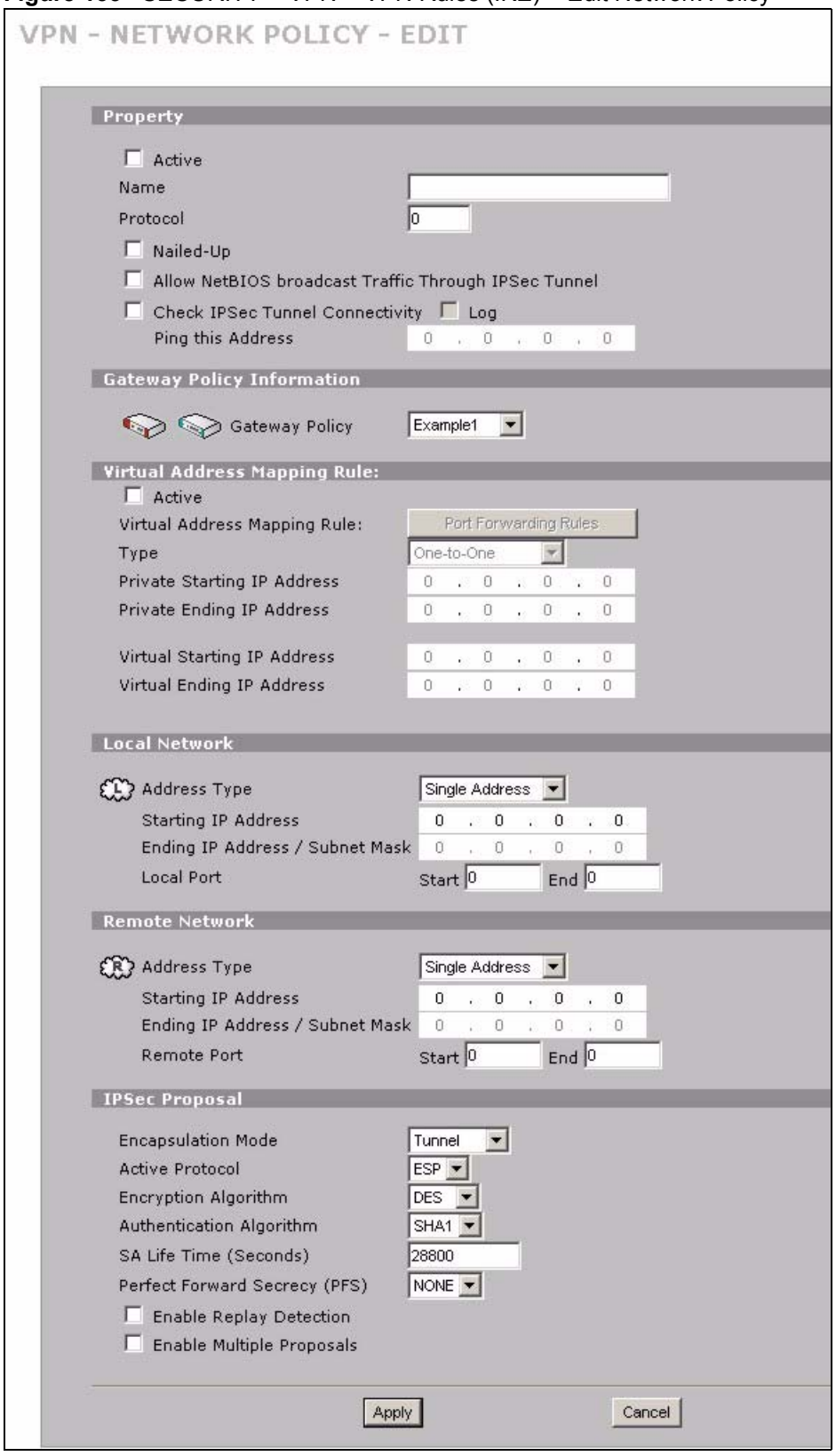
If you do not enable PFS, the ZyWALL and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

13.7 Network Policy Edit

Click **SECURITY > VPN** and the add network policy ( ) icon in the **VPN Rules (IKE)** screen to display the **VPN-Network Policy -Edit** screen. Use this screen to configure a network policy. A network policy identifies the devices behind the IPSec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.

Figure 133 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy



The following table describes the labels in this screen.

Table 63 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy

LABEL	DESCRIPTION
Active	If the **Active** check box is selected, packets for the tunnel trigger the ZyWALL to build the tunnel. Clear the **Active** check box to turn the network policy off. The ZyWALL does not apply the policy. Packets for the tunnel do not trigger the tunnel. If you clear the **Active** check box while the tunnel is up (and click **Apply**), you turn off the network policy and the tunnel goes down.
Name	Type a name to identify this VPN network policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Nailed-Up	Select this check box to turn on the nailed up feature for this SA. Turn on nailed up to have the ZyWALL automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The ZyWALL also reinitiates the SA when it restarts. The ZyWALL also rebuilds the tunnel if it was disconnected due to the output or input idle timer.
Allow NetBIOS Traffic Through IPSec Tunnel	This field is not available when the ZyWALL is in bridge mode. NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa. Select this check box to send NetBIOS packets through the VPN connection.
Check IPSec Tunnel Connectivity	Select the check box and configure an IP address in the **Ping this Address** field to have the ZyWALL periodically test the VPN tunnel to the remote IPSec router. The ZyWALL pings the IP address every minute. The ZyWALL starts the IPSec connection idle timeout timer when it sends the ping packet. If there is no traffic from the remote IPSec router by the time the timeout period expires, the ZyWALL disconnects the VPN tunnel.
Log	Select this check box to set the ZyWALL to create logs when it cannot ping the remote device.
Ping this Address	If you select **Check IPSec Tunnel Connectivity**, enter the IP address of a computer at the remote IPSec network. The computer's IP address must be in this IP policy's remote range (see the **Remote Network** fields).
Gateway Policy Information	
Gateway Policy	Select the gateway policy with which to use the VPN policy or store it in the recycle bin (without an association to any gateway policy).
Virtual Address Mapping Rule	Virtual address mapping over VPN is available with the routing and zero configuration modes.
Active	Enable this feature to have the ZyWALL use virtual (translated) IP addresses for the local network for the VPN connection. You do not configure the **Local Network** fields when you enable virtual address mapping. Virtual address mapping allows local and remote networks to have overlapping IP addresses. Virtual address mapping (NAT over IPSec) translates the source IP addresses of computers on your local network to other (virtual) IP addresses before sending the packets to the remote IPSec router. This translation hides the source IP addresses of computers in the local network.

Table 63 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy (continued)

LABEL	DESCRIPTION
Port Forwarding Rules	If you are configuring a **Many-to-One** rule, click this button to go to a screen where you can configure port forwarding for your VPN tunnels. The VPN network policy port forwarding rules let the ZyWALL forward traffic coming in through the VPN tunnel to the appropriate IP address.
Type	Select **One-to-One** to translate a single (static) IP address on your LAN to a single virtual IP address. Select **Many-to-One** to translate a range of (static) IP addresses on your LAN to a single virtual IP address. Many-to-one rules are for traffic going out from your LAN, through the VPN tunnel, to the remote network. Use port forwarding rules to allow incoming traffic from the remote network. Select **Many One-to-One** to translate a range of (static) IP addresses on your LAN to a range of virtual IP addresses.
Private Starting IP Address	Specify the IP addresses of the devices behind the ZyWALL that can use the VPN tunnel. When you select **One-to-One** in the **Type** field, enter the (static) IP address of a computer on the LAN behind your ZyWALL. When you select **Many-to-One** or **Many One-to-One** in the **Type** field, enter the beginning (static) IP address in a range of computers on the LAN behind your ZyWALL.
Private Ending IP Address	When you select **Many-to-One** or **Many One-to-One** in the **Type** field, enter the ending (static) IP address in a range of computers on the LAN behind your ZyWALL.
Virtual Starting IP Address	Enter the (static) IP addresses that represent the translated private IP addresses. These must correspond to the remote IPSec router's configured remote IP addresses. When you select **One-to-One** or **Many-to-One** in the **Type** field, enter an IP address as the translated IP address. Many-to-one rules are only for traffic going to the remote network. Use port forwarding rules to allow incoming traffic from the remote network. When you select **Many One-to-One** in the **Type** field, enter the beginning IP address of a range of translated IP addresses.
Virtual Ending IP Address	When you select **Many One-to-One** in the **Type** field, enter the ending (static) IP address of a range of translated IP addresses. The size of the private address range must be equal to the size of the translated virtual address range.
Local Network	Specify the IP addresses of the devices behind the ZyWALL that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses. You do not configure the **Local Network** fields when you enable virtual address mapping. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your ZyWALL.

Table 63 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy (continued)

LABEL	DESCRIPTION
Ending IP Address/ Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your ZyWALL.
Local Port	0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Remote Network	Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Address Type	Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the Addr Type field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router.
Ending IP Address/ Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router.
Remote Port	0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
IPSec Proposal	
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode.
Active Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase processing requirements and communications latency (delay).
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **NULL** - no encryption key or algorithm DES - a 56-bit key with the DES encryption algorithm 3DES - a 168-bit key with the DES encryption algorithm AES - a 128-bit key with the AES encryption algorithm The ZyWALL and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.

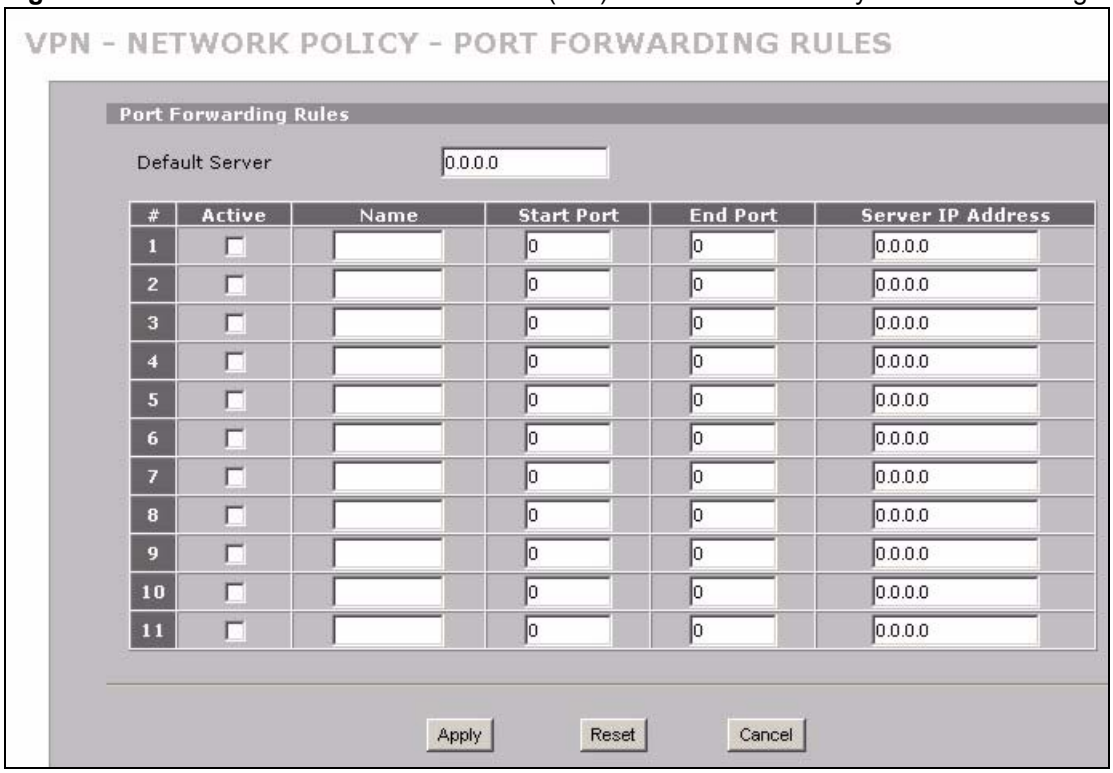
Table 63 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy (continued)

LABEL	DESCRIPTION
SA Life Time (Seconds)	Define the length of time before an IPSec SA automatically renegotiates in this field. The minimum value is 180 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **NONE** - disable PFS **DH1** - enable PFS and use a 768-bit random number **DH2** - enable PFS and use a 1024-bit random number **DH5** - enable PFS and use a 1536-bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by selecting this check box.
Enable Multiple Proposals	Select this to allow the ZyWALL to use any of its phase 2 encryption and authentication algorithms when negotiating an IPSec SA. When you enable multiple proposals, the ZyWALL allows the remote IPSec router to select which phase 2 encryption and authentication algorithms to use for the IPSec SA, even if they are less secure than the ones you configure for the VPN rule. Clear this to have the ZyWALL use only the configured phase 2 encryption and authentication algorithms when negotiating an IPSec SA.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard all changes and return to the main VPN screen.

13.8 Network Policy Port Forwarding

Click **SECURITY > VPN** and the add network policy ( ) icon in the **VPN Rules (IKE)** screen to display the **VPN-Network Policy -Edit** screen. Then, under **Virtual Address Mapping Rule**, select **Many-to-One** as the **Type** and click the **Port Forwarding Rules** button to open the following screen. Use this screen to configure port forwarding for your VPN tunnels to let the ZyWALL forward traffic coming in through the VPN tunnel to the appropriate IP address on the LAN.

Figure 134 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy > Port Forwarding



The following table describes the labels in this screen.

Table 64 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy > Port Forwarding

LABEL	DESCRIPTION
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, all packets received for ports not specified in this screen are discarded.
#	Number of an individual port forwarding server entry.
Active	Select this check box to activate the port forwarding server entry.
Name	Enter a descriptive name for identifying purposes.
Start Port	Type a port number in this field. To forward only one port, type the port number again in the **End Port** field. To forward a series of ports, type the start port number here and the end port number in the **End Port** field.
End Port	Type a port number in this field. To forward only one port, type the port number in the **Start Port** field above and then type it again in this field. To forward a series of ports, type the last port number in a series that begins with the port number in the **Start Port** field above.
Server IP Address	Type your server IP address in this field.
Apply	Click this button to save these settings.
Reset	Click this button to begin configuring this screen afresh.
Cancel	Click this button to return to the **VPN-Network Policy -Edit** screen without saving your changes.

13.9 Network Policy Move

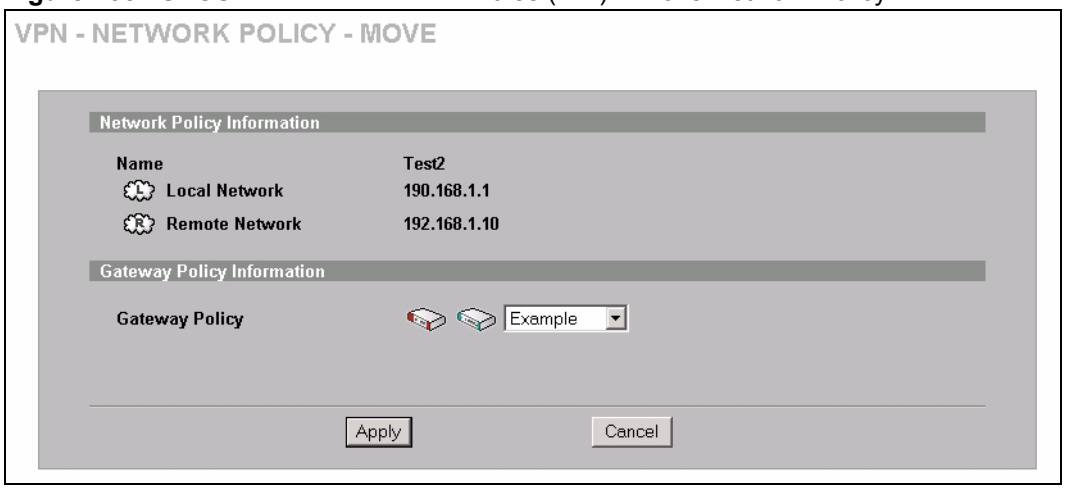
Click the move ( ) icon in the **VPN Rules (IKE)** screen to display the **VPN Rules (IKE): Network Policy Move** screen.

A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network. Each VPN tunnel uses a single gateway policy and one or more network policies.

- The gateway policy contains the IKE SA settings. It identifies the IPSec routers at either end of a VPN tunnel.
- The network policy contains the IPSec SA settings. It specifies which devices (behind the IPSec routers) can use the VPN tunnel.

Use this screen to associate a network policy to a gateway policy.

Figure 135 SECURITY > VPN > VPN Rules (IKE) > Move Network Policy



The following table describes the labels in this screen.

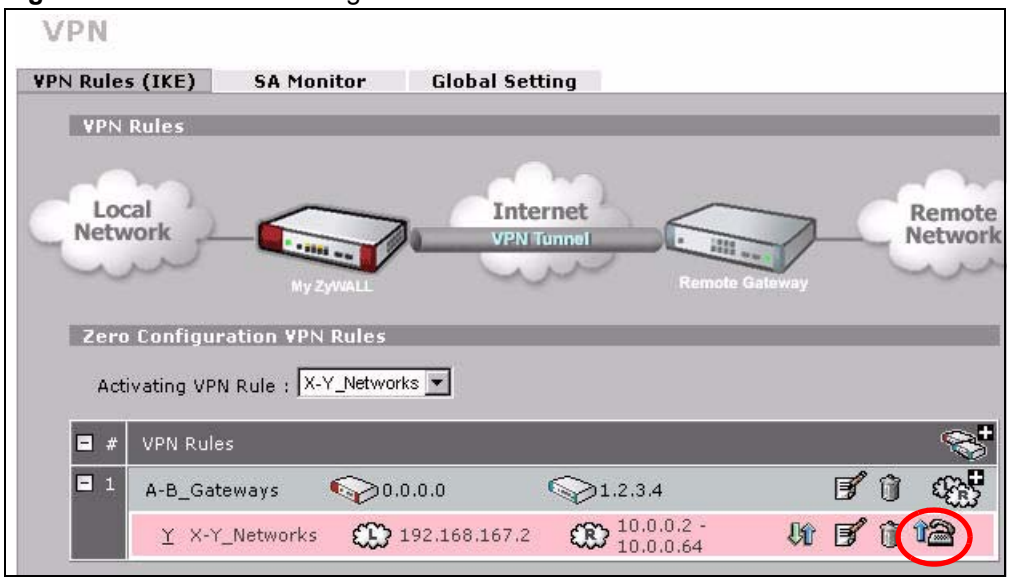
Table 65 SECURITY > VPN > VPN Rules (IKE) > Move Network Policy

LABEL	DESCRIPTION
Network Policy Information	The following fields display the general network settings of this VPN policy.
Name	This field displays the policy name.
Local Network	This field displays one or a range of IP address(es) of the computer(s) behind the ZyWALL.
Remote Network	This field displays one or a range of IP address(es) of the remote network behind the remote IPsec router.
Gateway Policy Information	
Gateway Policy	Select the name of a VPN rule (or gateway policy) to which you want to associate this VPN network policy. If you do not want to associate a network policy to any gateway policy, select **Recycle Bin** from the drop-down list box. The **Recycle Bin** gateway policy is a virtual placeholder for any network policy(ies) without an associated gateway policy. When there is a network policy in **Recycle Bin**, the **Recycle Bin** gateway policy automatically displays in the **VPN Rules (IKE)** screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard all changes and return to the main VPN screen.

13.10 Dialing the VPN Tunnel via Web Configurator

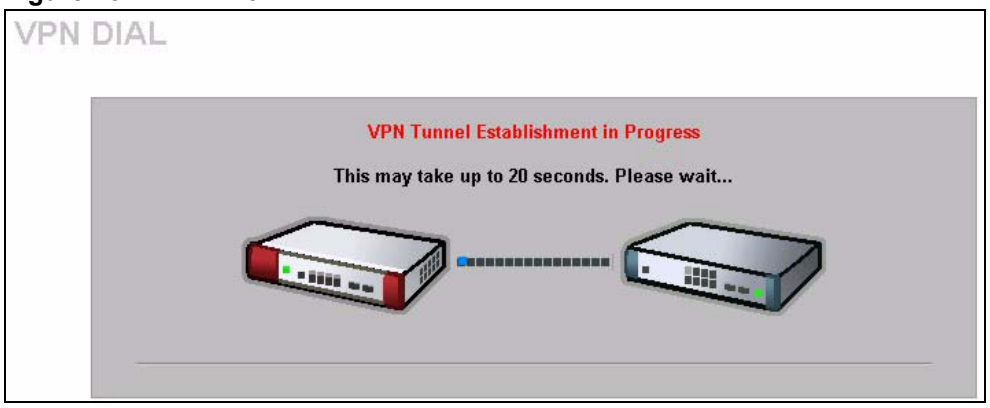
To test whether the IPSec routers can build the VPN tunnel, click the dial ( ) icon in the **VPN Rules (IKE)** screen to have the IPSec routers set up the tunnel.

Figure 136 VPN Rule Configured



The following screen displays.

Figure 137 VPN Dial



This screen displays later if the IPSec routers can build the VPN tunnel.

Figure 138 VPN Tunnel Established

13.11 IPSec Debug

If you are having difficulty building an IPSec tunnel to a non-ZyXEL IPSec router, advanced users may wish to examine the IPSec debug feature (in the commands).

If any of your VPN rules have an active network policy set to nailed-up, using the IPSec debug feature may cause the ZyWALL to continuously display new information. Type `ipsec debug level 0` and press [ENTER] to stop it.

Figure 139 IKE/IPSec Debug Example

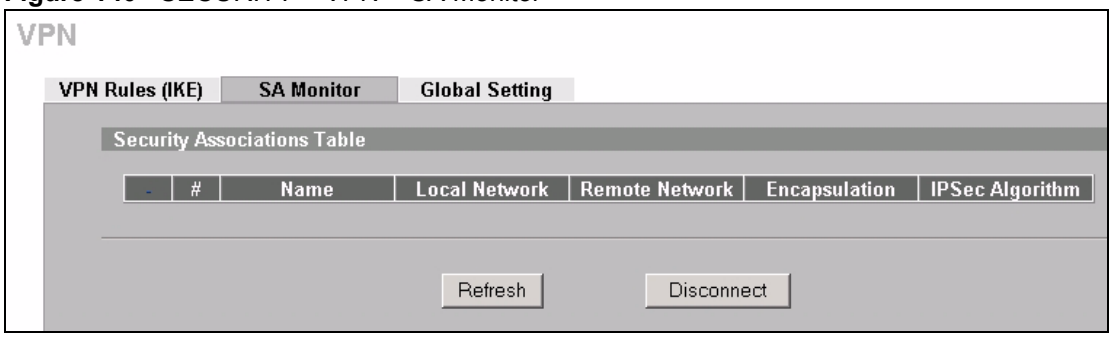
```
ras> ipsec debug
type            level           display
ras> ipsec debug type
<0:Disable | 1:Original on|off | 2:IKE on|off | 3: IPSec [SPI]|on|off |
4:XAUTH on|off | 5:CERT on|off | 6: All>
ras> ipsec debug level
<0:None | 1:User | 2:Low | 3:High>

ras> ipsec debug type 1 on
ras> ipsec debug type 2 on
ras> ipsec debug level 3

ras> ipsec dial 1
get_ipsec_sa_by_policyIndex():
Start dialing for tunnel <rule# 1>...
ikeStartNegotiate(): saIndex<0>
peerIp<5.1.2.3> protocol: <IPSEC_ESP>(3)

   peer Ip <5.1.2.3> initiator(): type<IPSEC_ESP>, exch<Main>

   initiator :
   protocol: IPSEC_ESP, exchange mode: Main mode  find_ipsec_sa():
      find ipsec saNot found

      Not found  isadb_is_outstanding_req():
      isakmp is outstanding req : SA not found
isadb_create_entry():  >> INITIATOR

  isadb_get_entry_by_addr():
      Get IKE entry by address:   SA not found

      SA not found  ISAKMP SA created for peer <BRANCH> size<900>

      ISAKMP SA created for peer <BRANCH> size<900>  ISAKMP SA built,
ikePeer.s0

      ISAKMP SA built, index = 0isadb_create_entry(): done

      create IKE entry doneinitiator(): find myIpAddr = 0.0.0.0, use
<5.6.7.8> r
```

13.12 VPN SA Monitor

In the web configurator, click **SECURITY > VPN > SA Monitor**. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections.

Figure 140 SECURITY > VPN > SA Monitor



The following table describes the labels in this screen.

Table 66 SECURITY > VPN > SA Monitor

LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Local Network	This field displays the IP address of the computer using the VPN IPSec feature of your ZyWALL.
Remote Network	This field displays IP address (in a range) of computers on the remote network behind the remote IPSec router.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase ZyWALL processing requirements and communications latency (delay).
Refresh	Click **Refresh** to display the current active VPN connection(s).
Disconnect	Select a security association index number that you want to disconnect and then click **Disconnect**.

13.13 VPN Global Setting

Click **SECURITY > VPN > Global Setting** to open the **VPN Global Setting** screen. Use this screen to change settings that apply to all of your VPN tunnels.

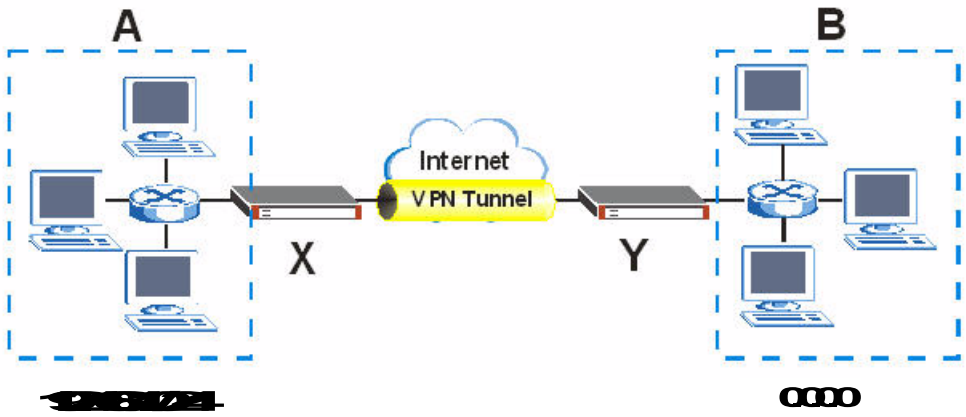
13.13.1 Local and Remote IP Address Conflict Resolution

Normally, you do not configure your local VPN policy rule's IP addresses to overlap with the remote VPN policy rule's IP addresses (see Section 13.6.2 on page 221). For example, you usually would not configure both with 192.168.1.0. However, overlapping local and remote network IP addresses can occur with dynamic VPN rules or IP alias.

13.13.1.1 Dynamic VPN Rule

Local and remote network IP addresses can overlap when you configure a dynamic VPN rule for a remote site (see Figure 141). For example, when you configure ZyWALL X, you configure the local network as 192.168.1.0/24 and the remote network as any (0.0.0.0). The "any" includes all possible IP addresses. It will forward traffic from network A to network B even if both the sender (for example 192.168.1.8) and the receiver (for example 192.168.1.9) are in network A. Note that the remote access can still use the VPN tunnel to access computers on ZyWALL X's network.

Figure 141 Overlap in a Dynamic VPN Rule



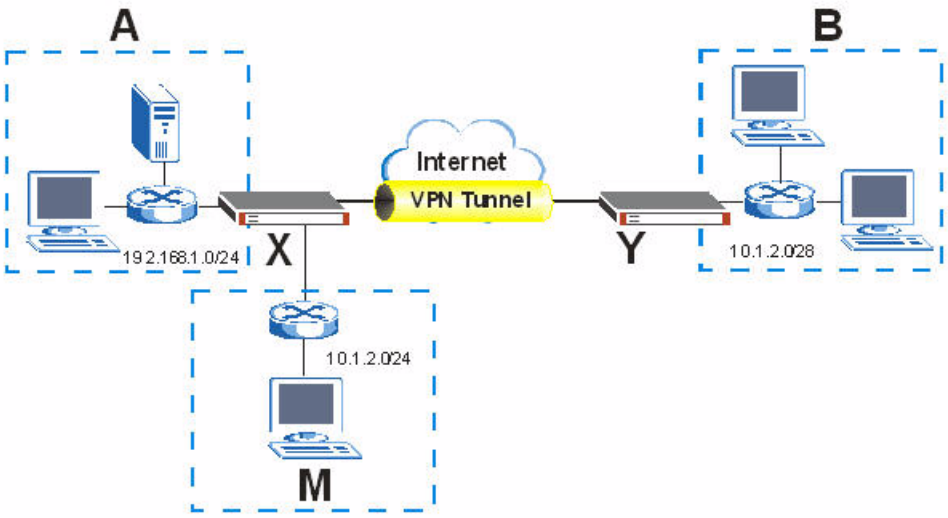
- Setting **Local and Remote IP Address Conflict Resolution** to **The Local Network** has the ZyWALL X check if a packet's destination is also at the local network before forwarding the packet. If it is, the ZyWALL sends the traffic to the local network.
- Setting **Local and Remote IP Address Conflict Resolution** to **The Remote Network** disables the checking for local network IP addresses.

13.13.1.2 IP Alias

You could have an IP alias network that overlaps with the VPN remote network (see Figure 142). For example, you have an IP alias network M (10.1.2.0/24) in ZyWALL X's LAN. For the VPN rule, you configure the VPN network as follows.

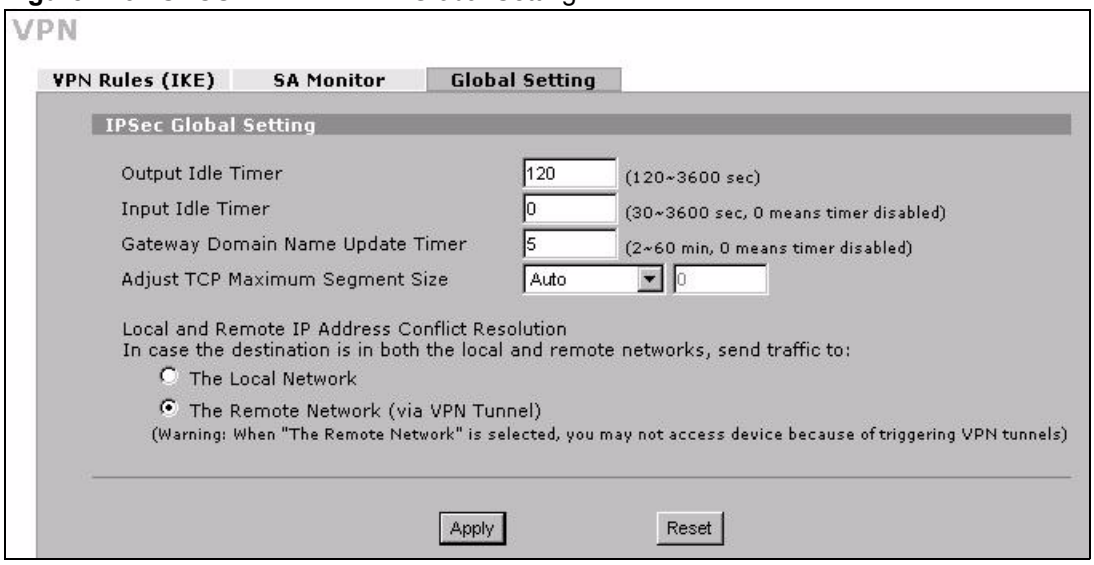
- Local IP address start: 192.168.1.1, end: 192.168.1.254
- Remote IP address start: 10.1.2.240, end: 10.1.2.254
- IP addresses 10.1.2.240 to 10.1.2.254 overlap.

Figure 142 Overlap in IP Alias and VPN Remote Networks



In this case, if you want to send packets from network A to an overlapped IP (ex. 10.1.2.241) that is in the IP alias network M, you have to set **Local and Remote IP Address Conflict Resolution** to **The Local Network**.

Figure 143 SECURITY > VPN > Global Setting


VPN
VPN Rules (IKE)
SA Monitor
Global Setting
IPSec Global Setting
Output Idle Timer
120
(120~3600 sec)
Input Idle Timer
0
(30~3600 sec, 0 means timer disabled)
Gateway Domain Name Update Timer
5
(2~60 min, 0 means timer disabled)
Adjust TCP Maximum Segment Size
Auto
0
Local and Remote IP Address Conflict Resolution
In case the destination is in both the local and remote networks, send traffic to:
The Local Network
The Remote Network (via VPN Tunnel)
(Warning: When "The Remote Network" is selected, you may not access device because of triggering VPN tunnels)
Apply
Reset

The following table describes the labels in this screen.

Table 67 SECURITY > VPN > Global Setting

LABEL	DESCRIPTION
Output Idle Timer	The ZyWALL disconnects a VPN tunnel if the remote IPSec router does not reply for this number of seconds.
Input Idle Timer	When no traffic is received from a remote IPSec router after the specified time period, the ZyWALL disconnects the VPN tunnel. **0** disables the check (this is the default setting). The output idle timer never takes affect if you set this timer to a shorter period.

Table 67 SECURITY > VPN > Global Setting (continued)

LABEL	DESCRIPTION
Gateway Domain Name Update Timer	If you use dynamic domain names in VPN rules to identify the ZyWALL and/or the remote IPSec router, the IP address mapped to the domain name can change. The VPN tunnel stops working after the IP address changes. Any users of the VPN tunnel are disconnected until the ZyWALL gets the new IP address from a DNS server and rebuilds the VPN tunnel. Enter the time period (between 2 and 60 minutes) to set how often the ZyWALL queries a DNS server to update the IP address and domain name mapping. If the query returns a new IP address for a dynamic domain name, the ZyWALL disconnects the VPN tunnel. The ZyWALL rebuilds the VPN tunnel (using the new IP address) immediately if the IPSec SA is set to nailed up. Otherwise the ZyWALL rebuilds the VPN tunnel when there are packets for it or you manually dial it. If the ZyWALL and all of the remote IPSec routers use static IP addresses or regular domain names, you can enter **0** to disable this feature.
Adjust TCP Maximum Segment Size	The TCP packets are larger after the ZyWALL encrypts them for VPN. The ZyWALL fragments packets that are larger than a connection's MTU (Maximum Transmit Unit). In most cases you should leave this set to **Auto**. The ZyWALL automatically sets the Maximum Segment Size (MSS) of the TCP packets that are to be encrypted by VPN based on the encapsulation type. Select **Off** to not adjust the MSS for the encrypted TCP packets. If your network environment causes fragmentation issues that are affecting your throughput performance, you can manually set a smaller MSS for the TCP packets that are to be encrypted by VPN. Select **User-Defined** and specify a size from 0~1460 bytes. 0 has the ZyWALL use the auto setting.
Local and Remote IP Address Conflict Resolution	Select **The Local Network** to send packets destined for overlapping local and remote IP addresses to the local network (you can access the local devices but not the remote devices). Select **The Remote Network (via VPN Tunnel)** to send packets destined for overlapping local and remote IP addresses to the remote network (you can access the remote devices but not the local devices.) If the remote IPSec router also supports NAT over IPSec, it is recommended that you use NAT over IPSec (see Section 13.6.2 on page 221) if the local and remote IP addresses overlap. If a VPN rule's local and remote network settings are both set to 0.0.0.0 (any), no traffic goes through the VPN tunnel if you select **The Local Network**.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

13.14 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single ZyWALL at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The ZyWALL at headquarters has a static public IP address.

13.14.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (**A**, **B** and **C** in the figure) to use one VPN rule to simultaneously access a ZyWALL at headquarters (**HQ** in the figure). The telecommuters do not have domain names mapped to the WAN IP addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

Figure 144 Telecommuters Sharing One VPN Rule Example

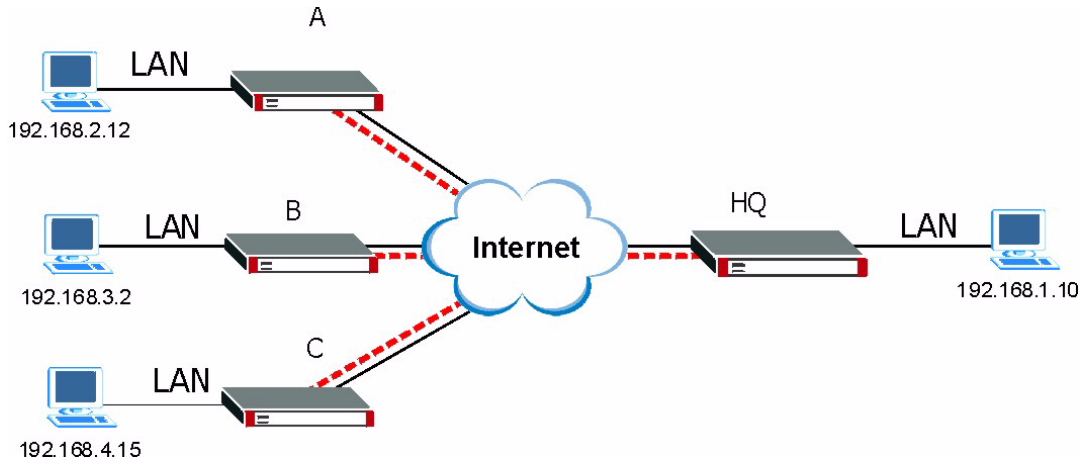


Table 68 Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
My ZyWALL:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Primary Remote Address:	Public static IP address	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.
Local Network - Single IP Address:	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15	192.168.1.10
Remote Network - Single IP Address:	192.168.1.10	Not Applicable

13.14.2 Telecommuters Using Unique VPN Rules Example

In this example the telecommuters (A, B and C in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see Section 13.3.1.4 on page 211), the ZyWALL can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a ZyWALL at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the ZyWALL at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a ZyWALL located at headquarters. The ZyWALL at headquarters (HQ in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The ZyWALL at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

Figure 145 Telecommuters Using Unique VPN Rules Example

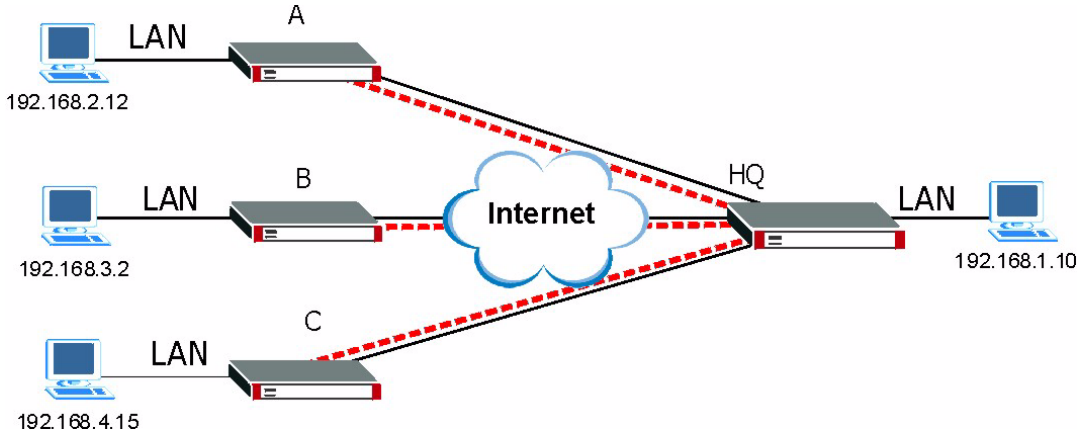


Table 69 Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
All Telecommuter Rules:	All Headquarters Rules:
My ZyWALL 0.0.0.0	My ZyWALL: bigcompanyhq.com
Primary Remote Address: bigcompanyhq.com	Local Network - Single IP Address: 192.168.1.10
Remote Network - Single IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	
Telecommuter A (telecommutera.dydns.org)	Headquarters ZyWALL Rule 1:
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Primary Remote Address: telecommutera.dydns.org
	Remote Address 192.168.2.12
Telecommuter B (telecommuterb.dydns.org)	Headquarters ZyWALL Rule 2:
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Primary Remote Address: telecommuterb.dydns.org
	Remote Address 192.168.3.2

Table 69 Telecommuters Using Unique VPN Rules Example

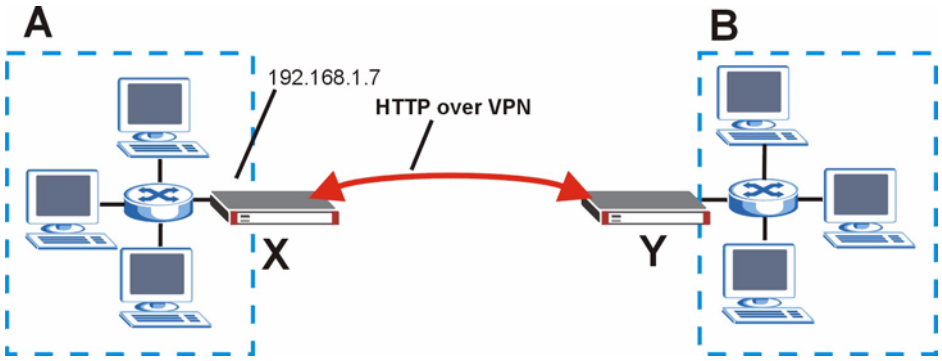
TELECOMMUTERS	HEADQUARTERS
Telecommuter C (telecommuterc.dydns.org)	Headquarters ZyWALL Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com
Local IP Address: 192.168.4.15	Primary Remote Address: telecommuterc.dydns.org
	Remote Address 192.168.4.15

13.15 VPN and Remote Management

You can allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the ZyWALL. One of the ZyWALL's ports must be part of the VPN rule's local network. This can be the ZyWALL's LAN port if you do not want to allow remote management on the WAN port. You also have to configure remote management (**REMOTE MGMT**) to allow management access for the service through the specific port.

In the following example, the VPN rule's local network (A) includes the ZyWALL's LAN IP address of 192.168.1.7. Someone in the remote network (B) can use a service (like HTTP for example) through the VPN tunnel to access the ZyWALL's LAN interface. Remote management must also be configured to allow HTTP access on the ZyWALL's LAN interface.

Figure 146 VPN for Remote Management Example



14

Certificates

This chapter gives background information about public-key certificates and explains how to use them.

14.1 Certificates Overview

The ZyWALL can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyWALL to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyWALL uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyWALL does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyWALL can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

14.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The ZyWALL only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

14.2 Self-signed Certificates

You can have the ZyWALL act as a certification authority and sign its own certificates.

14.3 Verifying a Certificate

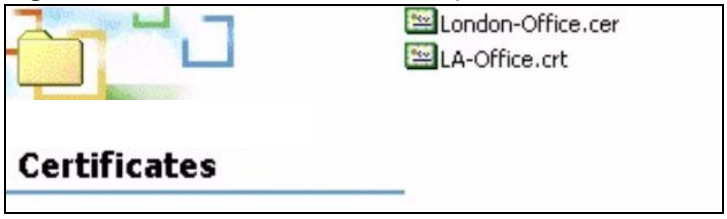
Before you import a trusted CA or trusted remote host certificate into the ZyWALL, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the ZyWALL also trusts any valid certificate signed by any of the imported trusted CA certificates.

14.3.1 Checking the Fingerprint of a Certificate on Your Computer

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

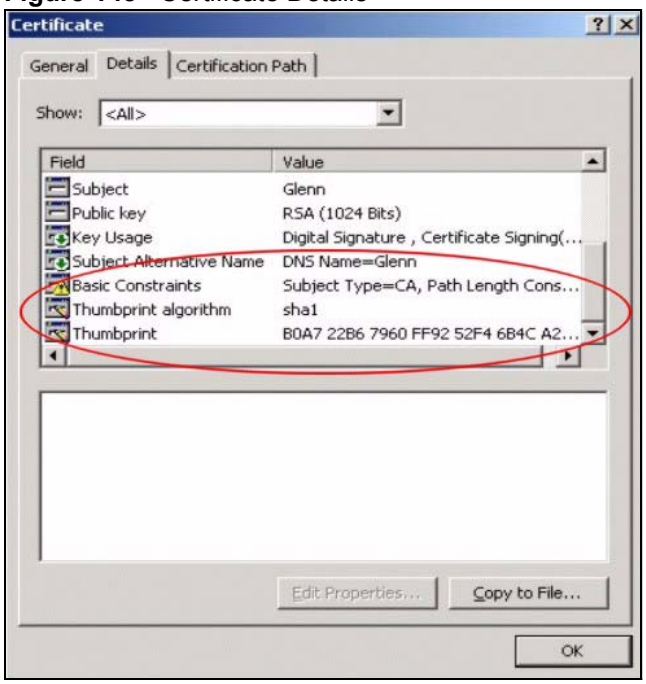
1. Browse to where you have the certificate saved on your computer.
2. Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 147 Certificates on Your Computer



3. Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 148 Certificate Details

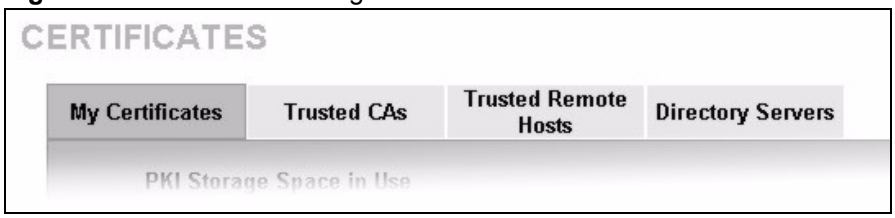


4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

14.4 Configuration Summary

This section summarizes how to manage certificates on the ZyWALL.

Figure 149 Certificate Configuration Overview



Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the ZyWALL's CA-signed certificates.

Use the **Trusted CA** screens to save the certificates of trusted CAs to the ZyWALL. You can also export the certificates to a computer.

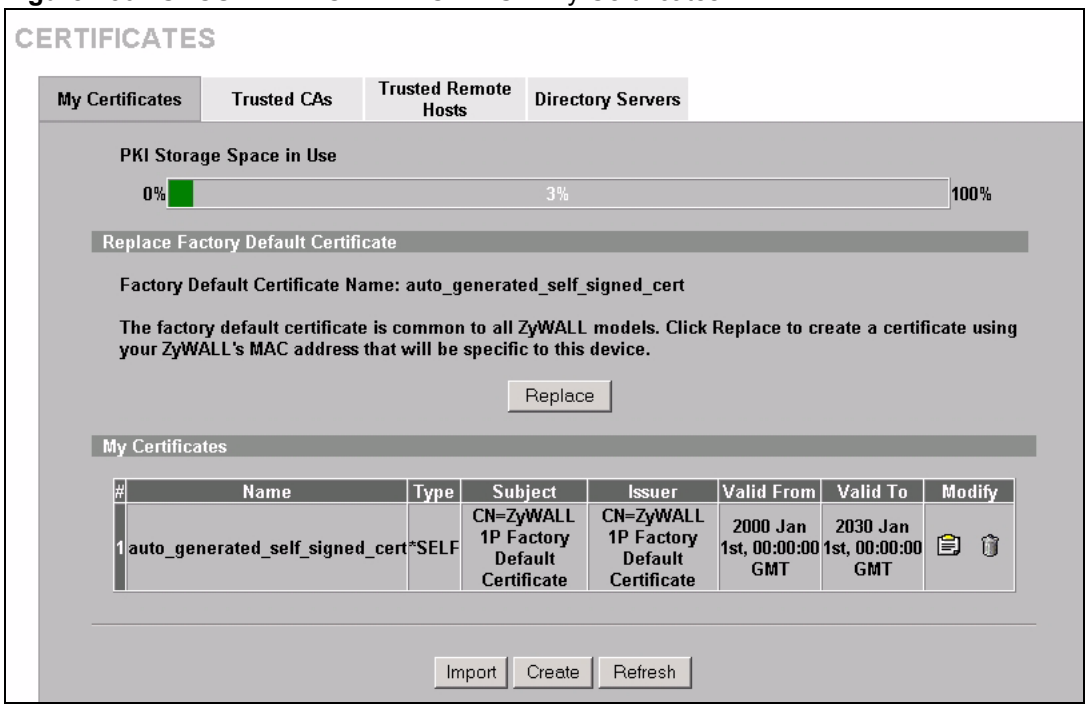
Use the **Trusted Remote Hosts** screens to import self-signed certificates from trusted remote hosts.

Use the **Directory Servers** screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

14.5 My Certificates

Click **SECURITY > CERTIFICATES > My Certificates** to open the **My Certificates** screen. This is the ZyWALL's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray.

Figure 150 SECURITY > CERTIFICATES > My Certificates


CERTIFICATES
My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers
PKI Storage Space in Use
0%
3%
100%
Replace Factory Default Certificate
Factory Default Certificate Name: auto_generated_self_signed_cert
The factory default certificate is common to all ZyWALL models. Click Replace to create a certificate using your ZyWALL's MAC address that will be specific to this device.
Replace
My Certificates
Name Type Subject Issuer Valid From Valid To Modify
1 auto_generated_self_signed_cert *SELF CN=ZyWALL 1P Factory Default Certificate CN=ZyWALL 1P Factory Default Certificate 2000 Jan 1st, 00:00:00 GMT 2030 Jan 1st, 00:00:00 GMT
Import
Create
Refresh

The following table describes the labels in this screen.

Table 70 SECURITY > CERTIFICATES > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the ZyWALL has the factory default certificate. The factory default certificate is common to all ZyWALLs that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyWALL's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. **REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request. **SELF** represents a self-signed certificate. ***SELF** represents the default self-signed certificate, which the ZyWALL uses to sign imported trusted remote host certificates. **CERT** represents a certificate issued by a certification authority.

Table 70 SECURITY > CERTIFICATES > My Certificates (continued)

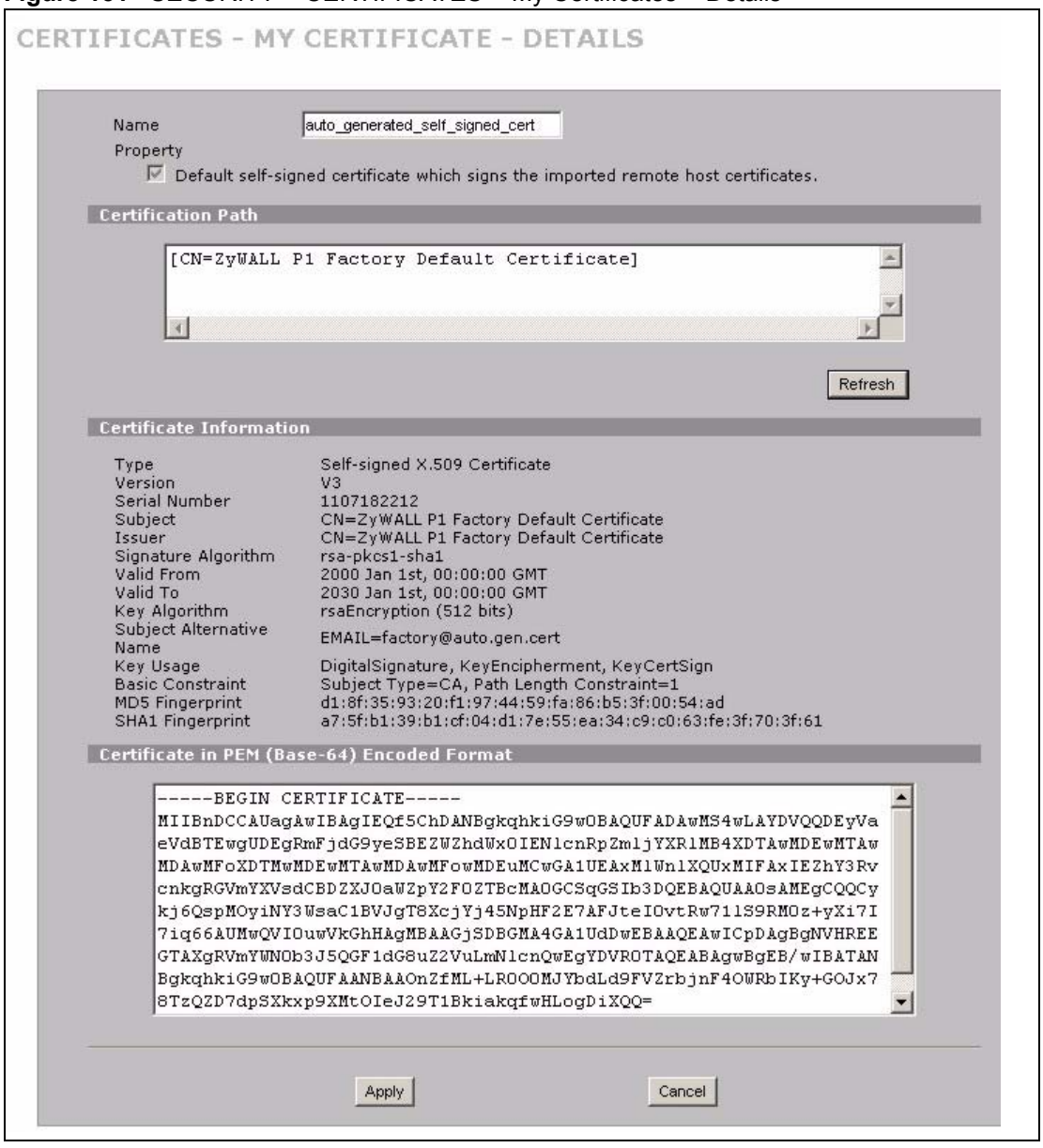
LABEL	DESCRIPTION
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the export icon to save the certificate to a computer. For a certification request, click the export icon and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. Click the delete icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate. You cannot delete a certificate that one or more features is configured to use. Do the following to delete a certificate that shows ***SELF** in the **Type** field. 1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the ***SELF** certificate. 2. Click the details icon next to another self-signed certificate (see the description on the **Create** button if you need to create a self-signed certificate). 3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box. 4. Click **Apply** to save the changes and return to the **My Certificates** screen. 5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now. Note that subsequent certificates move up by one when you take this action
Import	Click **Import** to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyWALL.
Create	Click **Create** to go to the screen where you can have the ZyWALL generate a certificate or a certification request.
Refresh	Click **Refresh** to display the current validity status of the certificates.

14.6 My Certificate Details

Click **SECURITY** > **CERTIFICATES** > **My Certificates** to open the **My Certificates** screen (see Figure 150 on page 246). Click the details icon to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

If it is a self-signed certificate, you can also set the ZyWALL to use the certificate to sign the imported trusted remote host certificates.

Figure 151 SECURITY > CERTIFICATES > My Certificates > Details



The following table describes the labels in this screen.

Table 71 SECURITY > CERTIFICATES > My Certificates > Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyWALL use this certificate to sign the trusted remote host certificates that you import to the ZyWALL. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.

Table 71 SECURITY > CERTIFICATES > My Certificates > Details (continued)

LABEL	DESCRIPTION
Certification Path	Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyWALL does not trust the certificate and displays “Not trusted” in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate’s owner signed the certificate (not a certification authority). “X.509” means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate’s identification number given by the certification authority or generated by the ZyWALL.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate’s issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyWALL uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate’s key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner‘s IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate’s key can be used. For example, “DigitalSignature” means that the key can be used to sign certificates and “KeyEncipherment” means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority’s certificate and “Path Length Constraint=1” means that there can only be one certification authority in the certificate’s path.
MD5 Fingerprint	This is the certificate’s message digest that the ZyWALL calculated using the MD5 algorithm.

Table 71 SECURITY > CERTIFICATES > My Certificates > Details (continued)

LABEL	DESCRIPTION
SHA1 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Apply	Click **Apply** to save your changes back to the ZyWALL. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

14.7 My Certificate Export

Click **SECURITY > CERTIFICATES > My Certificates** and then a certificate's export icon to open the **My Certificate Export** screen. Follow the instructions in this screen to choose the file format to use for saving the certificate from the ZyWALL to a computer.

14.7.1 Certificate File Export Formats

You can export a certificate in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the ZyWALL.

Figure 152 SECURITY > CERTIFICATES > My Certificates > Export

CERTIFICATES - MY CERTIFICATE - EXPORT
Export
Please specify whether to export the certificate along with the corresponding private key.
Export the certificate in binary X.509 format.
Export the certificate along with the corresponding private key in PKCS#12 format.
For security concern, you may provide a password to protect the private key.
Password
Retype to Confirm
Apply
Cancel

The following table describes the labels in this screen.

Table 72 SECURITY > CERTIFICATES > My Certificates > Export

LABEL	DESCRIPTION
Export the certificate in binary X.509 format.	Binary X.509 is an ITU-T recommendation that defines the formats for X.509 certificates.
Export the certificate along with the corresponding private key in PKCS#12 format.	PKCS#12 is a format for transferring public key and private key certificates. You can also password-encrypt the private key in the PKCS #12 file. The file's password is not connected to your certificate's public or private passwords.
Password	Type the file's password to use for encrypting the private key. The password is optional, although you must specify one if you want to be able to import the PKCS#12 format certificate into Netscape version 7.2.
Retype to confirm	Type the password to make sure that you have entered it correctly.
Apply	Click **Apply** and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

14.8 My Certificate Import

Click **SECURITY > CERTIFICATES > My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate from a computer to the ZyWALL.

- You can only import a certificate that matches a corresponding certification request that was generated by the ZyWALL (the certification request contains the private key). The certificate you import replaces the corresponding request in the My Certificates screen. One exception is that you can import a PKCS#12 format certificate without a corresponding certification request since the certificate includes the private key.
- You must remove any spaces from the certificate's filename before you can import it.

14.8.1 Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyWALL currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the ZyWALL.

Be careful to not convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

Figure 153 SECURITY > CERTIFICATES > My Certificates > Import

CERTIFICATES - MY CERTIFICATE - IMPORT
Import
Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.
Binary X.509
PEM (Base-64) encoded X.509
Binary PKCS#7
PEM (Base-64) encoded PKCS#7
Binary PKCS#12
PEM (Base-64) encoded PKCS#12
For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted.
File Path:
Browse...
Apply
Cancel

The following table describes the labels in this screen.

Table 73 SECURITY > CERTIFICATES > My Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the ZyWALL.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

When you import a binary PKCS#12 format certificate, another screen displays for you to enter the password.

Figure 154 SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12

The following table describes the labels in this screen.

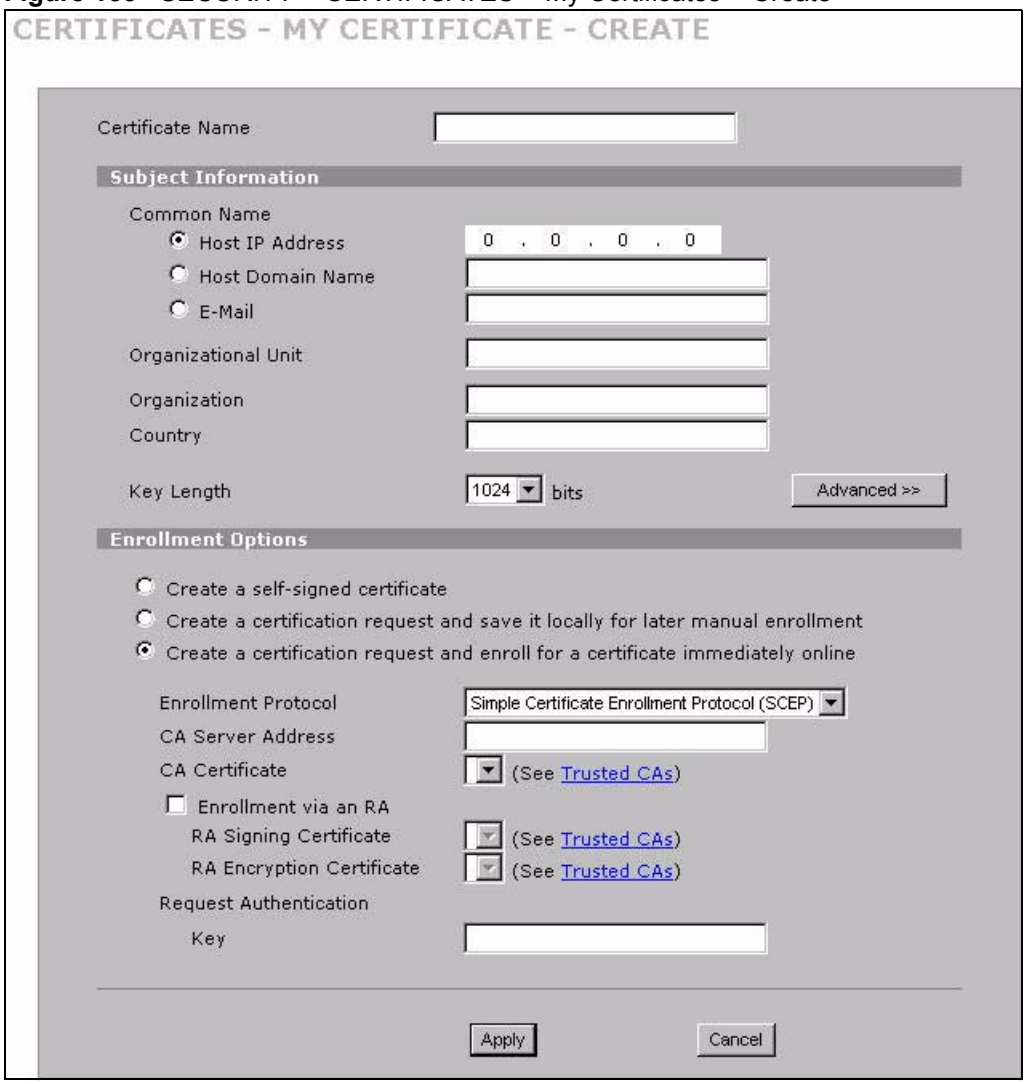
Table 74 SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12

LABEL	DESCRIPTION
Password	Type the file's password that was created when the PKCS #12 file was exported.
Apply	Click **Apply** to save the certificate on the ZyWALL.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

14.9 My Certificate Create

Click **SECURITY** > **CERTIFICATES** > **My Certificates > Create** to open the **My Certificate Create** screen. Use this screen to have the ZyWALL create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 155 SECURITY > CERTIFICATES > My Certificates > Create



The following table describes the labels in this screen.

Table 75 SECURITY > CERTIFICATES > My Certificates > Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the **Common Name** is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyWALL drops trailing spaces.

Table 75 SECURITY > CERTIFICATES > My Certificates > Create (continued)

LABEL	DESCRIPTION
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select **Create a self-signed certificate** to have the ZyWALL generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select **Create a certification request and save it locally for later manual enrollment** to have the ZyWALL generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (see Section 14.6 on page 247) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select **Create a certification request and enroll for a certificate immediately online** to have the ZyWALL generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the **CA Certificate** drop-down list box. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyWALL's list of certificates of trusted certification authorities.
Enrollment via an RA	If you select **Create a certification request and enroll for a certificate immediately online**, you can select this option to apply for a certificate through a RA (Registration Authority). The RA is an intermediary authorized by a CA to verify each subscriber's identity and forward the requests to the CA. After the CA signs and issues the certificates, the RA distributes the certificates to the subscribers.

Table 75 SECURITY > CERTIFICATES > My Certificates > Create (continued)

LABEL	DESCRIPTION
RA Signing Certificate	If you select **Enrollment via an RA**, select the CA's RA signing certificate from the drop-down list box. You must have the certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyWALL's list of certificates of trusted certification authorities.
RA Encryption Certificate	If you select **Enrollment via an RA**, select the CA's RA encryption certificate from the drop-down list box. You must have the certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyWALL's list of certificates of trusted certification authorities.
Request Authentication	When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just fill in the **Key** field if your certification authority uses the SCEP enrollment protocol.
Key	Type the key that the certification authority gave you. You can use up to 31 ASCII printable characters. Spaces are allowed.
Apply	Click **Apply** to begin certificate or certification request generation.
Cancel	Click **Cancel** to quit and return to the **My Certificates** screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyWALL is generating the self-signed certificate or certification request.

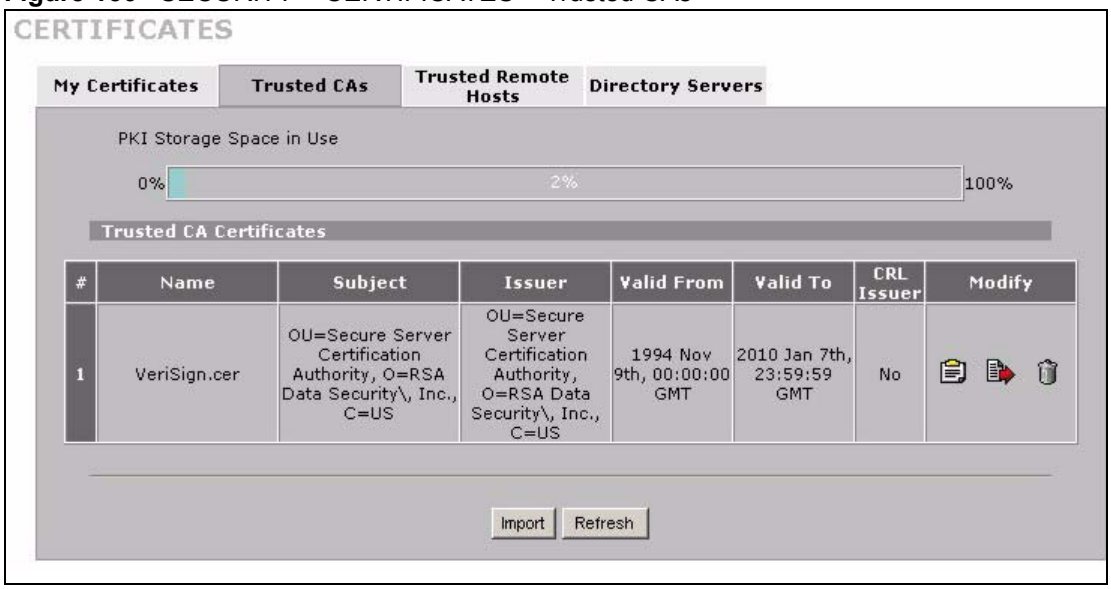
After the ZyWALL successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyWALL enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyWALL to enroll a certificate online.

14.10 Trusted CAs

Click **SECURITY** > **CERTIFICATES** > **Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyWALL to accept as trusted. The ZyWALL accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 156 SECURITY > CERTIFICATES > Trusted CAs


CERTIFICATES
My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers
PKI Storage Space in Use
0%
2%
100%
Trusted CA Certificates
Name Subject Issuer Valid From Valid To CRL Issuer Modify
1 VeriSign.cer OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US 1994 Nov 9th, 00:00:00 GMT 2010 Jan 7th, 23:59:59 GMT No
Import
Refresh

The following table describes the labels in this screen.

Table 76 SECURITY > CERTIFICATES > Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the **Issues certificate revocation lists (CRL)** check box in the certificate's details screen to have the ZyWALL check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".

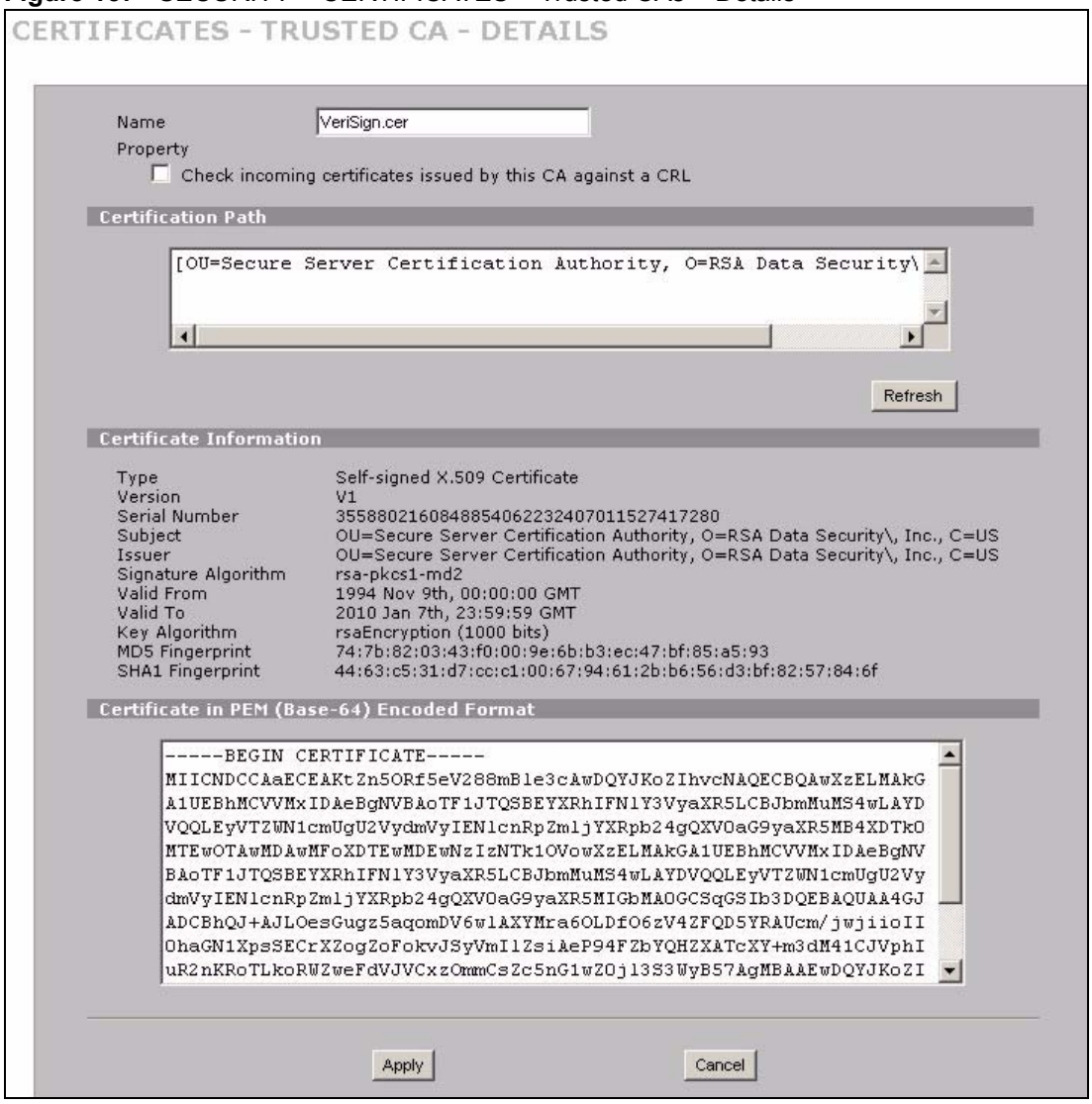
Table 76 SECURITY > CERTIFICATES > Trusted CAs (continued)

LABEL	DESCRIPTION
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Use the export icon to save the certificate to a computer. Click the icon and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyWALL.
Refresh	Click this button to display the current validity status of the certificates.

14.11 Trusted CA Details

Click **SECURITY** > **CERTIFICATES** > **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyWALL to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 157 SECURITY > CERTIFICATES > Trusted CAs > Details



The following table describes the labels in this screen.

Table 77 SECURITY > CERTIFICATES > Trusted CAs > Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Check incoming certificates issued by this CA against a CRL	Select this check box to have the ZyWALL check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this check box to have the ZyWALL not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).

Table 77 SECURITY > CERTIFICATES > Trusted CAs > Details (continued)

LABEL	DESCRIPTION
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyWALL does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the **Subject Name** field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.

Table 77 SECURITY > CERTIFICATES > Trusted CAs > Details (continued)

LABEL	DESCRIPTION
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Apply	Click **Apply** to save your changes back to the ZyWALL. You can only change the name and/or set whether or not you want the ZyWALL to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

14.12 Trusted CA Import

Click **SECURITY** > **CERTIFICATES** > **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate from a computer to the ZyWALL. The ZyWALL trusts any valid certificate signed by any of the imported trusted CA certificates.

You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 158 SECURITY > CERTIFICATES > Trusted CAs > Import

CERTIFICATES - TRUSTED CA - IMPORT
Import
Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.
Binary X.509
PEM (Base-64) encoded X.509
Binary PKCS#7
PEM (Base-64) encoded PKCS#7
File Path:
Browse...
Apply
Cancel

The following table describes the labels in this screen.

Table 78 SECURITY > CERTIFICATES > Trusted CAs Import

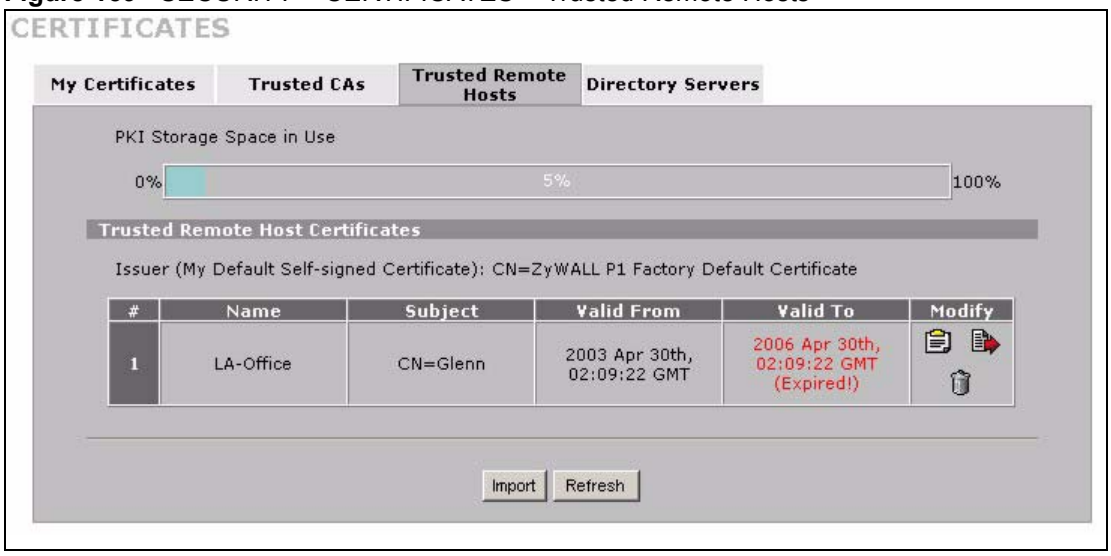
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the ZyWALL.
Cancel	Click **Cancel** to quit and return to the **Trusted CAs** screen.

14.13 Trusted Remote Hosts

Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. This screen displays a list of the certificates of peers that you trust but which are not signed by one of the certification authorities on the **Trusted CAs** screen.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the ZyWALL automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

Figure 159 SECURITY > CERTIFICATES > Trusted Remote Hosts



The following table describes the labels in this screen.

Table 79 SECURITY > CERTIFICATES > Trusted Remote Hosts

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Issuer (My Default Self-signed Certificate)	This field displays identifying information about the default self-signed certificate on the ZyWALL that the ZyWALL uses to sign the trusted remote host certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Use the export icon to save the certificate to a computer. Click the icon and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.
Import	Click **Import** to open a screen where you can save the certificate of a remote host (which you trust) from your computer to the ZyWALL.
Refresh	Click this button to display the current validity status of the certificates.

14.14 Trusted Remote Hosts Import

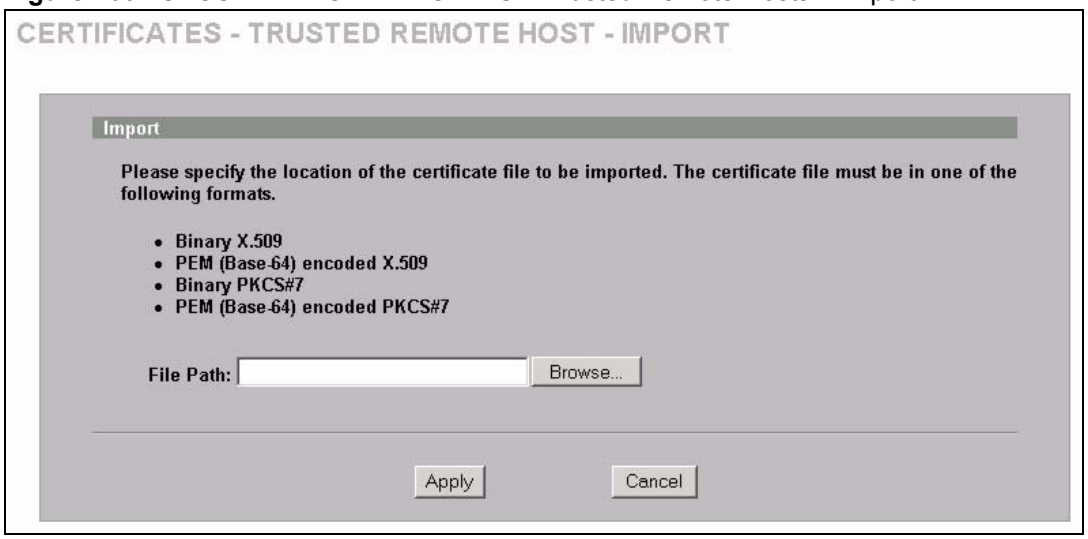
Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen.

You may have peers with certificates that you want to trust, but the certificates were not signed by one of the certification authorities on the **Trusted CAs** screen. Follow the instructions in this screen to save a peer's certificates from a computer to the ZyWALL.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the ZyWALL automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

The trusted remote host certificate must be a self-signed certificate; and you must remove any spaces from its filename before you can import it.

Figure 160 SECURITY > CERTIFICATES > Trusted Remote Hosts > Import


CERTIFICATES - TRUSTED REMOTE HOST - IMPORT
Import
Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.
Binary X.509
PEM (Base-64) encoded X.509
Binary PKCS#7
PEM (Base-64) encoded PKCS#7
File Path:
Browse...
Apply
Cancel

The following table describes the labels in this screen.

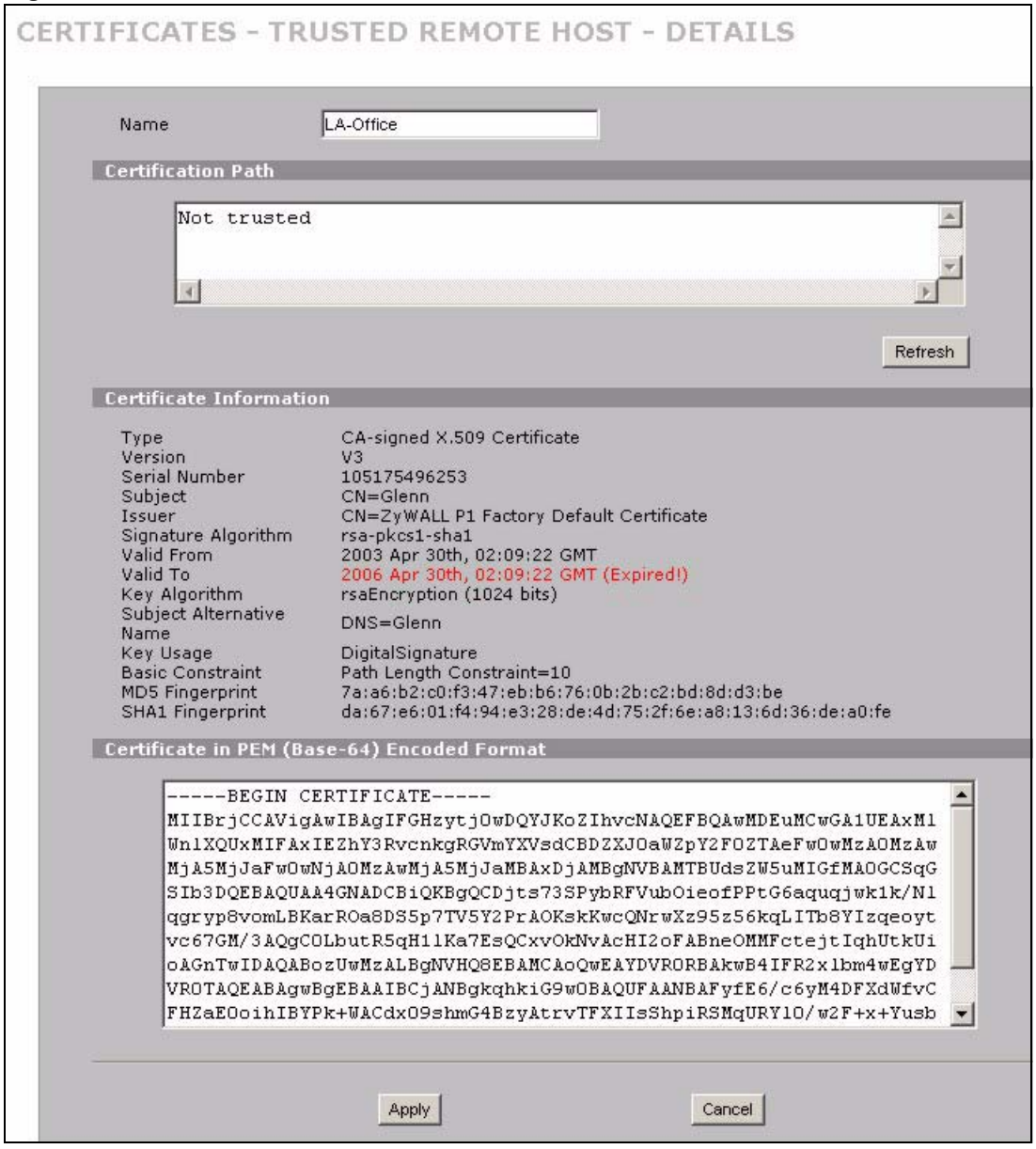
Table 80 SECURITY > CERTIFICATES > Trusted Remote Hosts > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the ZyWALL.
Cancel	Click **Cancel** to quit and return to the **Trusted Remote Hosts** screen.

14.15 Trusted Remote Host Certificate Details

Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. Click the details icon to open the **Trusted Remote Host Details** screen. You can use this screen to view in-depth information about the trusted remote host's certificate and/or change the certificate's name.

Figure 161 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details



The following table describes the labels in this screen.

Table 81 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certification Path	Click the **Refresh** button to have this read-only text box display the end entity's own certificate and a list of certification authority certificates in the hierarchy of certification authorities that validate a certificate's issuing certification authority. For a trusted host, the list consists of the end entity's own certificate and the default self-signed certificate that the ZyWALL uses to sign remote host certificates.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. With trusted remote host certificates, this field always displays CA-signed. The ZyWALL is the Certification Authority that signed the certificate. X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the device that created the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the default self-signed certificate on the ZyWALL that the ZyWALL uses to sign the trusted remote host certificates.
Signature Algorithm	This field displays the type of algorithm that the ZyWALL used to sign the certificate, which is rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.

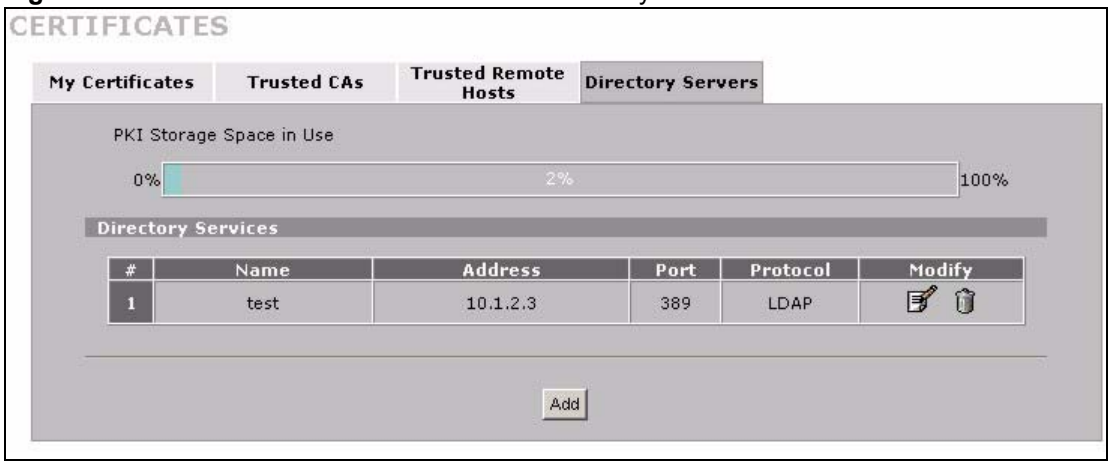
Table 81 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details (continued)

LABEL	DESCRIPTION
MD5 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm. The ZyWALL uses one of its own self-signed certificates to sign the imported trusted remote host certificates. This changes the fingerprint value displayed here (so it does not match the original). See Section 14.3 on page 244 for how to verify a remote host's certificate before you import it into the ZyWALL.
SHA1 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm. The ZyWALL uses one of its own self-signed certificates to sign the imported trusted remote host certificates. This changes the fingerprint value displayed here (so it does not match the original). See Section 14.3 on page 244 for how to verify a remote host's certificate before you import it into the ZyWALL.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Apply	Click **Apply** to save your changes back to the ZyWALL. You can only change the name of the certificate.
Cancel	Click **Cancel** to quit configuring this screen and return to the **Trusted Remote Hosts** screen.

14.16 Directory Servers

Click **SECURITY** > **CERTIFICATES** > **Directory Servers** to open the **Directory Servers** screen. This screen displays a summary list of directory servers (that contain lists of valid and revoked certificates) that have been saved into the ZyWALL. If you decide to have the ZyWALL check incoming certificates against the issuing certification authority's list of revoked certificates, the ZyWALL first checks the server(s) listed in the **CRL Distribution Points** field of the incoming certificate. If the certificate does not list a server or the listed server is not available, the ZyWALL checks the servers listed here.

Figure 162 SECURITY > CERTIFICATES > Directory Servers



The following table describes the labels in this screen.

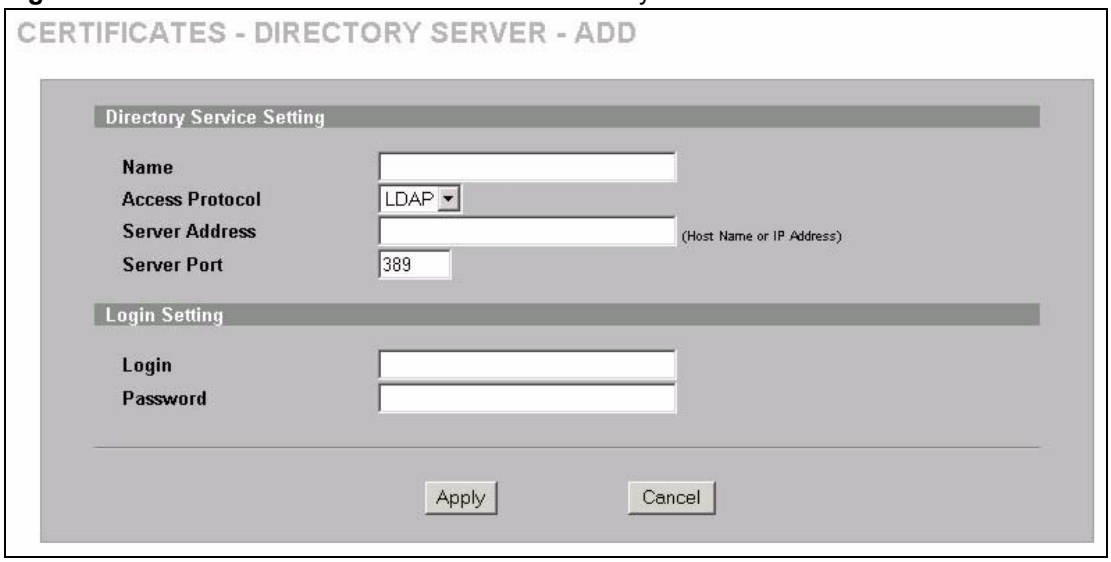
Table 82 SECURITY > CERTIFICATES > Directory Servers

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	The index number of the directory server. The servers are listed in alphabetical order.
Name	This field displays the name used to identify this directory server.
Address	This field displays the IP address or domain name of the directory server.
Port	This field displays the port number that the directory server uses.
Protocol	This field displays the protocol that the directory server uses.
Modify	Click the details icon to open a screen where you can change the information about the directory server. Click the delete icon to remove the directory server entry. A window displays asking you to confirm that you want to delete the directory server. Note that subsequent certificates move up by one when you take this action.
Add	Click **Add** to open a screen where you can configure information about a directory server so that the ZyWALL can access it.

14.17 Directory Server Add or Edit

Click **SECURITY > CERTIFICATES > Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to open the **Directory Server Add** screen. Use this screen to configure information about a directory server that the ZyWALL can access.

Figure 163 SECURITY > CERTIFICATES > Directory Server > Add



The following table describes the labels in this screen.

Table 83 SECURITY > CERTIFICATES > Directory Server > Add

LABEL	DESCRIPTION
Directory Service Setting	
Name	Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server.
Access Protocol	Use the drop-down list box to select the access protocol used by the directory server. **LDAP** (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.[A]
Server Address	Type the IP address (in dotted decimal notation) or the domain name of the directory server.
Server Port	This field displays the default server port number of the protocol that you select in the **Access Protocol** field. You may change the server port number if needed, however you must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
Login Setting	
Login	The ZyWALL may need to authenticate itself in order to assess the directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to quit configuring this screen and return to the **Directory Servers** screen.

A. At the time of writing, LDAP is the only choice of directory server access protocol.

15

Authentication Server

This chapter discusses how to configure the ZyWALL's authentication server feature.

15.1 Authentication Server Overview

A ZyWALL set to be a VPN extended authentication server can use either the local user database internal to the ZyWALL or an external RADIUS (Remote Authentication Dial In User Service) server for an unlimited number of users. The ZyWALL uses the local user database for VPN extended authentication.

15.1.1 Local User Database

By storing user profiles locally on the ZyWALL, your ZyWALL is able to authenticate users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

15.1.2 RADIUS

The ZyWALL can use an external RADIUS server to authenticate an unlimited number of users. A RADIUS server enables user authentication, authorization and accounting. RADIUS is based on a client-sever model that supports authentication and accounting, where access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks among others:

- Authentication
  Determines the identity of the users.
- Accounting
  Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which your ZyWALL acts as a message relay between the user and the network RADIUS server. See RFC 2138 and RFC 2139 for more on RADIUS.

15.1.2.1 Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
  Sent by an access point requesting authentication.
- **Access-Reject**

Sent by a RADIUS server rejecting access.

- **Access-Accept**
  Sent by a RADIUS server allowing access.
- **Access-Challenge**
  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

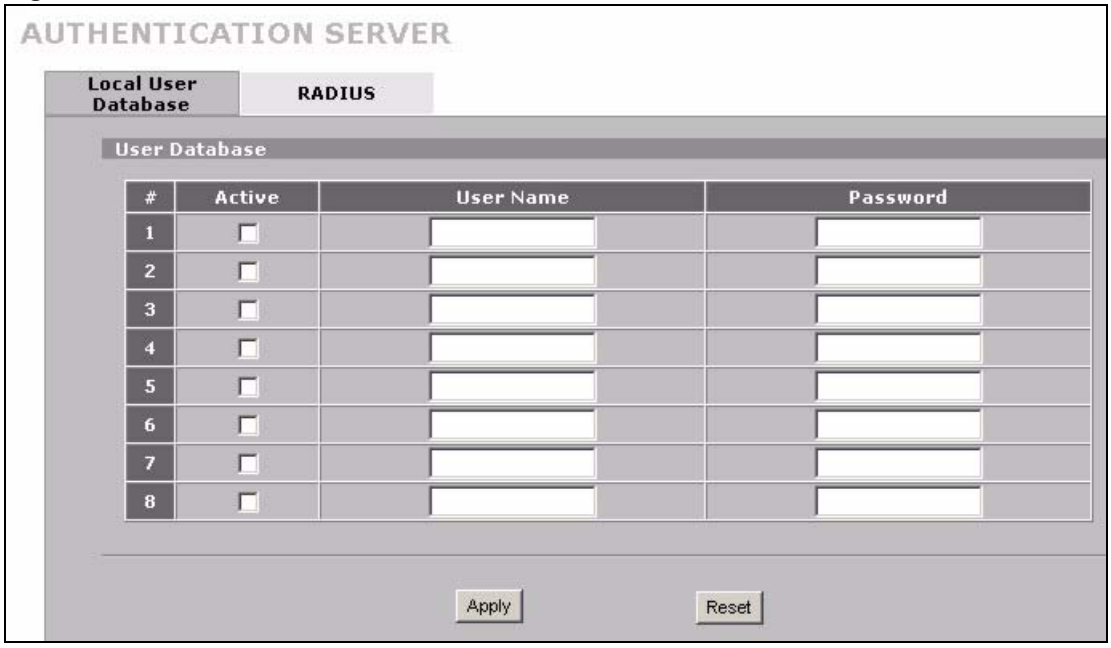
- **Accounting-Request**
  Sent by the access point requesting accounting.
- **Accounting-Response**
  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

15.2 Local User Database

Click **SECURITY** > **AUTH SERVER** to open the **Local User Database** screen. The local user database is a list of user profiles stored on the ZyWALL. The ZyWALL can use this list of user profiles to authenticate users. Use this screen to change your ZyWALL's list of user profiles.

Figure 164 SECURITY > AUTH SERVER > Local User Database



The following table describes the labels in this screen.

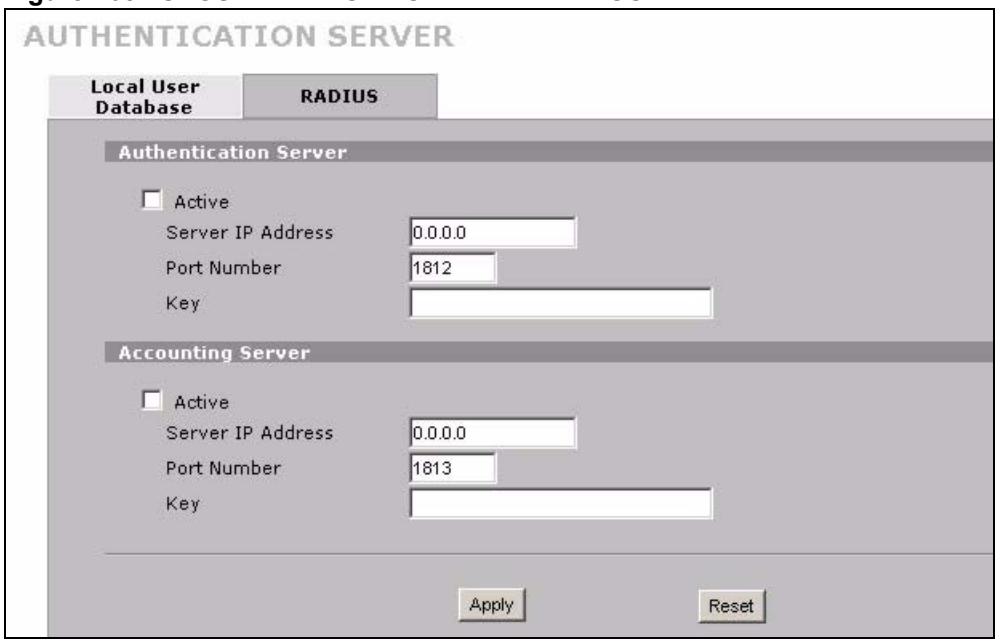
Table 84 SECURITY > AUTH SERVER > Local User Database

LABEL	DESCRIPTION
Active	Select this check box to enable the user profile.
User Name	Enter the user name of the user profile.
Password	Enter a password up to 31 characters long for this user profile.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

15.3 RADIUS

Click **SECURITY** > **AUTH SERVER** > **RADIUS** to open the **RADIUS** screen. Configure this screen to use an external RADIUS server to authenticate users.

Figure 165 SECURITY > AUTH SERVER > RADIUS



The following table describes the labels in this screen.

Table 85 SECURITY > AUTH SERVER > RADIUS

LABEL	DESCRIPTION
Authentication Server	
Active	Select the check box to enable user authentication through an external authentication server. Clear the check box to enable user authentication using the local user profile on the ZyWALL.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.

Table 85 SECURITY > AUTH SERVER > RADIUS

LABEL	DESCRIPTION
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyWALL. The key is not sent over the network. This key must be the same on the external authentication server and ZyWALL.
Accounting Server	
Active	Select the check box to enable user accounting through an external authentication server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyWALL. The key is not sent over the network. This key must be the same on the external accounting server and ZyWALL.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

PART IV
Advanced

Network Address Translation (NAT) (277)
Static Route (293)
Remote Management (297)
UPnP (319)
Custom Application (329)
ALG Screen (331)

16

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

16.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

16.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyWALL. For example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router. For example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 86 NAT Definitions

TERM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

16.1.2 What NAT Does

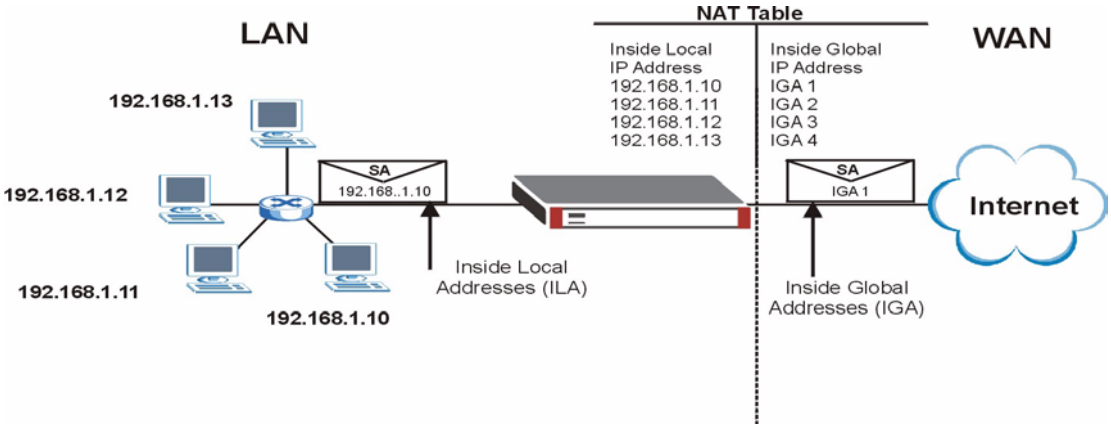
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyWALL filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

16.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyWALL keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

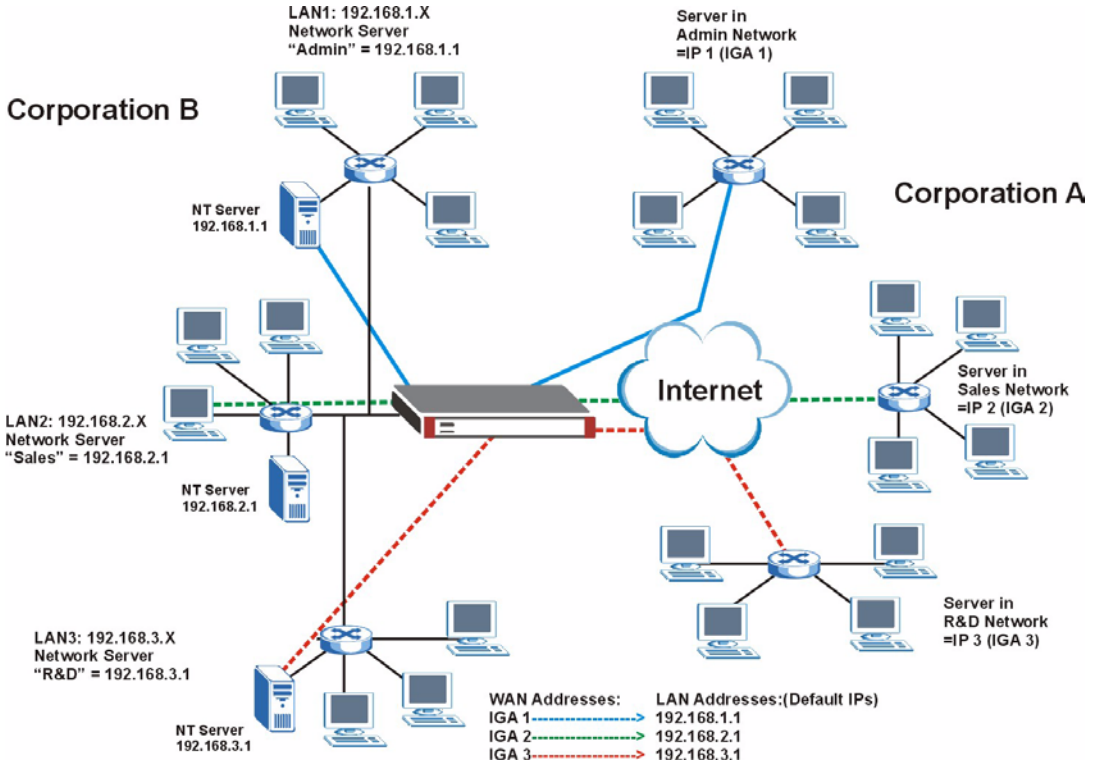
Figure 166 How NAT Works



16.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyWALL can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 167 NAT Application With IP Alias



16.1.5 Port Restricted Cone NAT

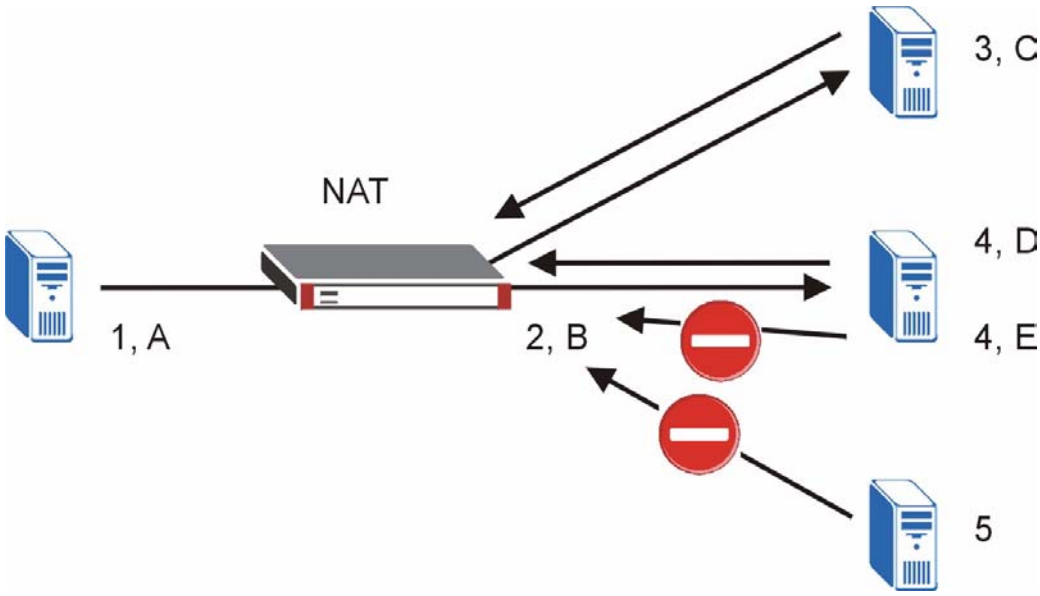
ZyWALL ZyNOS version 4.00 and later uses port restricted cone NAT. Port restricted cone NAT maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the ZyWALL maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. A host on the external network (IP address **3** and Port **C** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address and port.

A server with IP address **1** and port **A** sends packets to IP address **3**, port **C** and IP address **4**, port **D**. The ZyWALL changes the server's IP address to **2** and port to **B**.

Since **1**, **A** has already sent packets to **3**, **C** and **4**, **D,** they can send packets back to **2**, **B** and the ZyWALL will perform NAT on them and send them to the server at IP address **1**, port **A**.

Packets have not been sent from **1**, **A** to **4**, **E** or **5**, so they cannot send packets to **1**, **A**.

Figure 168 Port Restricted Cone NAT Example



16.1.6 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the ZyWALL maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyWALL maps multiple local IP addresses to one global IP address. This is equivalent to SUA (that is, PAT, port address translation), ZyXEL's Single User Account feature (the **SUA** option).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyWALL maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One**: In Many-One-to-One mode, the ZyWALL maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do not change for One-to-One and Many-One-to-One NAT mapping types.

The following table summarizes the NAT mapping types.

Table 87 NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1 < > IGA1
Many-to-One (SUA/PAT)	ILA1 < > I IGA1 ILA2 < > I IGA1 …

Table 87 NAT Mapping Types

TYPE	IP MAPPING
Many-to-Many Overload	ILA1 < > I IGA1 ILA2 < > IGA2 ILA3 < > IGA1 ILA4 < > IGA2 …
Many-One-to-One	ILA1 < > IGA1 ILA2 < > IGA2 ILA3 < > IGA3 …
Server	Server 1 IP < > IGA1 Server 2 IP < > IGA1 Server 3 IP < > IGA1

16.2 Using NAT

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyWALL.

16.2.1 SUA (Single User Account) Versus NAT

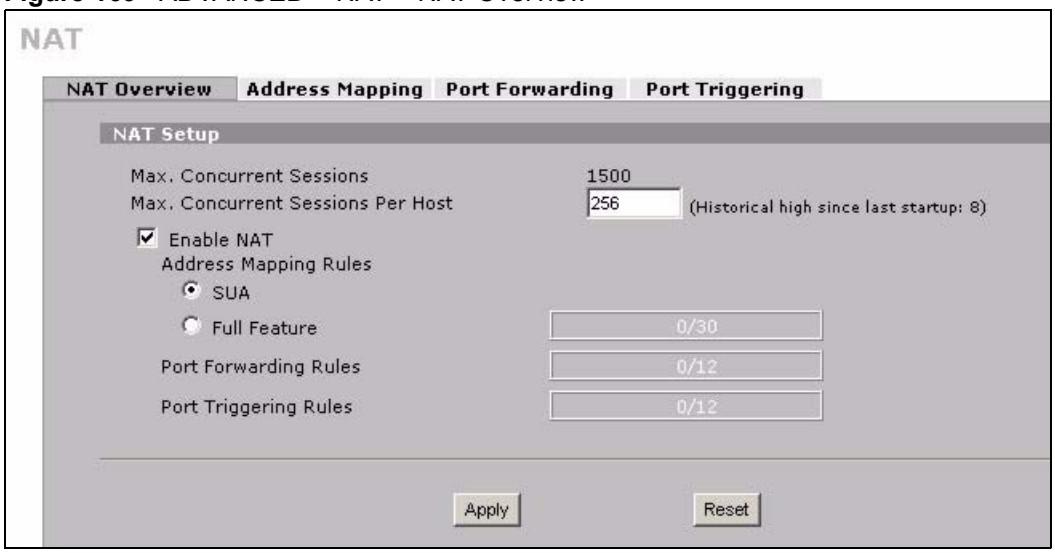
SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyWALL also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA** or **Full Feature** in **NAT Overview**.

Selecting **SUA** means (latent) multiple WAN-to-LAN address translation.

16.3 NAT Overview Screen

Click **ADVANCED > NAT** to open the **NAT Overview** screen.

Figure 169 ADVANCED > NAT > NAT Overview



The following table describes the labels in this screen.

Table 88 ADVANCED > NAT > NAT Overview

LABEL	DESCRIPTION
Max. Concurrent Sessions	This read-only field displays the highest number of NAT sessions that the ZyWALL will permit at one time.
Max. Concurrent Sessions Per Host	When computers use peer to peer applications, such as file sharing applications, they need to establish NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet. Use this field to set the highest number of NAT sessions that the ZyWALL will permit a host to have at one time. If your network has one or two clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has more users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions.
Enable NAT	Select this check box to turn on the NAT feature for the WAN port. Clear this check box to turn off the NAT feature for the WAN port.
Address Mapping Rules	Select **SUA** if you have just one public WAN IP address for your ZyWALL. This lets the ZyWALL use its permanent, pre-defined NAT address mapping rules. Select **Full Feature** if you have multiple public WAN IP addresses for your ZyWALL. This lets the ZyWALL use the address mapping rules that you configure. This is the equivalent of what used to be called full feature NAT or multi-NAT. Note: Full feature address mapping is available while the ZyWALL is in routing mode. The bar displays how many of the ZyWALL's possible address mapping rules are configured. The first number shows how many address mapping rules are configured on the ZyWALL. The second number shows the maximum number of address mapping rules that can be configured on the ZyWALL.

Table 88 ADVANCED > NAT > NAT Overview (continued)

LABEL	DESCRIPTION
Port Forwarding Rules	The bar displays how many of the ZyWALL's possible port forwarding rules are configured. The first number shows how many port forwarding rules are configured on the ZyWALL. The second number shows the maximum number of port forwarding rules that can be configured on the ZyWALL.
Port Triggering Rules	The bar displays how many of the ZyWALL's possible trigger port rules are configured. The first number shows how many trigger port rules are configured on the ZyWALL. The second number shows the maximum number of trigger port rules that can be configured on the ZyWALL.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

16.4 NAT Address Mapping

Click **ADVANCED** > **NAT** > **Address Mapping** to open the following screen.

Full feature address mapping is available while the ZyWALL is in routing mode.

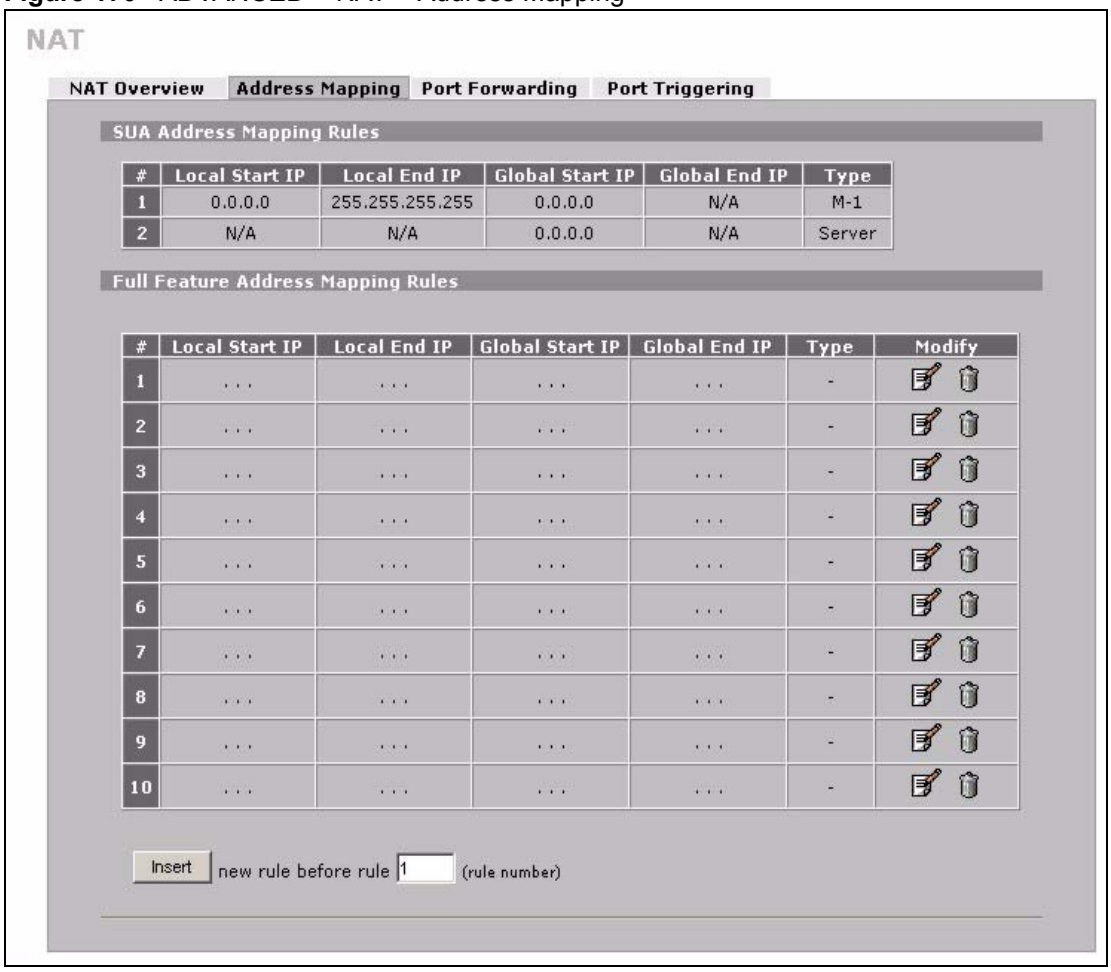
16.4.1 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

Use this screen to change your ZyWALL's address mapping settings. See Section 16.1 on page 277 for more on NAT.

Ordering your rules is important because the ZyWALL applies the rules in the order that you specify. When a rule matches the current packet, the ZyWALL takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

Figure 170 ADVANCED > NAT > Address Mapping


NAT
NAT Overview
Address Mapping
Port Forwarding
Port Triggering
SUA Address Mapping Rules
Local Start IP Local End IP Global Start IP Global End IP Type
1 0.0.0.0 255.255.255.255 0.0.0.0 N/A M-1
2 N/A N/A 0.0.0.0 N/A Server
Full Feature Address Mapping Rules
Local Start IP Local End IP Global Start IP Global End IP Type Modify
1 . . . . -
2 . . . . -
3 . . . . -
4 . . . . -
5 . . . . -
6 . . . . -
7 . . . . -
8 . . . . -
9 . . . . -
10 . . . . -
Insert
new rule before rule 1
(rule number)

The following table describes the labels in this screen.

Table 89 ADVANCED > NAT > Address Mapping

LABEL	DESCRIPTION
SUA Address Mapping Rules	This read-only table displays the default address mapping rules.
Full Feature Address Mapping Rules	
#	This is the rule index number.
Local Start IP	This refers to the Inside Local Address (ILA), which is the starting local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA), that is the starting global IP address. 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types.

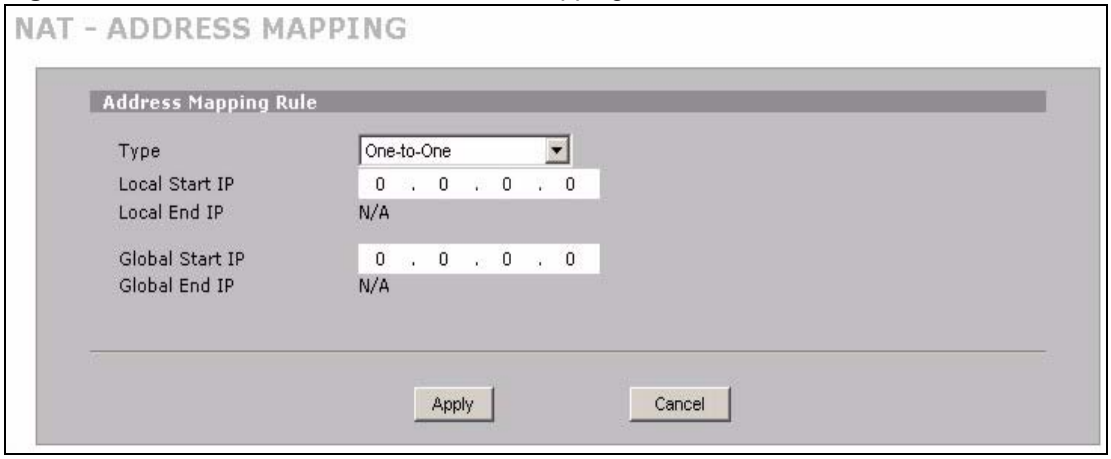
Table 89 ADVANCED > NAT > Address Mapping (continued)

LABEL	DESCRIPTION
Global End IP	This is the ending Inside Global Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Type	1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type. 2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (that is, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. 3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One** mode maps each local IP address to unique global IP addresses. 5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. A window display asking you to confirm that you want to delete the address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.
Insert	Click **Insert** to insert a new mapping rule before an existing one.

16.4.2 NAT Address Mapping Edit

Click the edit button to display the **NAT Address Mapping Edit** screen. Use this screen to edit an address mapping rule. See Section 16.1 on page 277 for information on NAT and address mapping.

Figure 171 ADVANCED > NAT > Address Mapping > Edit



The following table describes the labels in this screen.

Table 90 ADVANCED > NAT > Address Mapping > Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. 1. **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-One NAT mapping type. 2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (that is, PAT, port address translation), ZyXEL's Single User Account feature. 3. **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One**: Many One-to-One mode maps each local IP address to unique global IP addresses. 5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter **0.0.0.0** here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

16.5 Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

16.5.1 Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

If you do not assign a default server IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

16.5.2 Port Forwarding: Services and Port Numbers

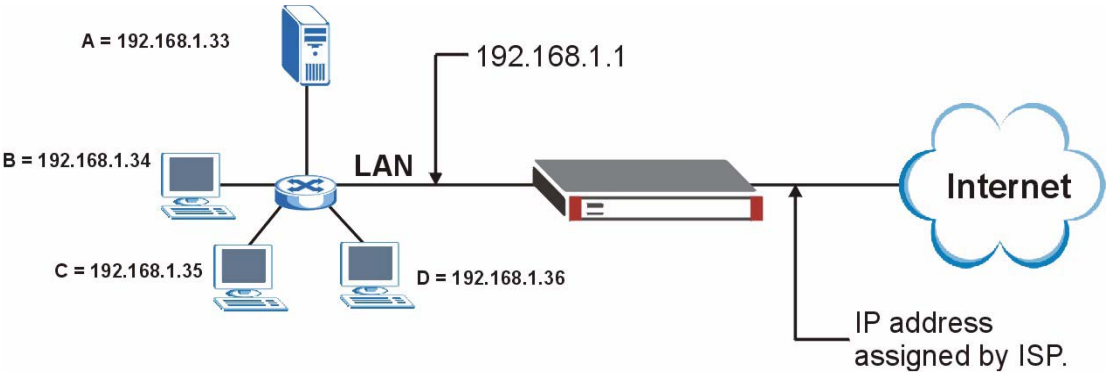
Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

The most often used port numbers are shown in Appendix D on page 463. Please refer to the user's guide and RFC 1700 for further information about port numbers.

16.5.3 Configuring Servers Behind Port Forwarding (Example)

In this example, you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the figure), port 80 to another (**B** in the figure) and assign a default server IP address of 192.168.1.35 to a third (**C** in the figure). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 172 Multiple Servers Behind NAT Example



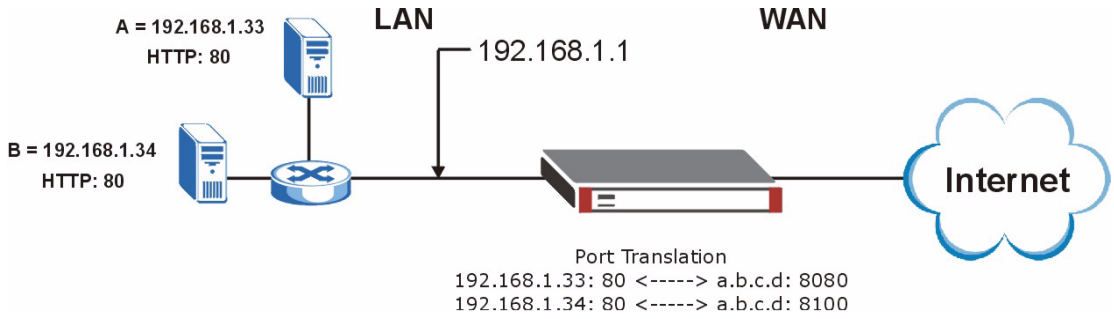
16.5.4 Port Translation

The ZyWALL can translate the destination port number or a range of port numbers of packets coming from the WAN to another destination port number or range of port numbers on the local network. When you use port forwarding without port translation, a single server on the local network can use a specific port number and be accessible to the outside world through a single WAN IP address. When you use port translation with port forwarding, multiple servers on the local network can use the same port number and still be accessible to the outside world through a single WAN IP address.

The following example has two web servers on a LAN. Server **A** uses IP address 192.168.1.33 and server **B** uses 192.168.1.34. Both servers use port 80. The letters a.b.c.d represent the WAN port's IP address. The ZyWALL translates port 8080 of traffic received on the WAN port (IP address a.b.c.d) to port 80 and sends it to server **A** (IP address 192.168.1.33). The ZyWALL also translates port 8100 of traffic received on the WAN port (also IP address a.b.c.d) to port 80, but sends it to server **B** (IP address 192.168.1.34).

In this example, anyone wanting to access server **A** from the Internet must use port 8080. Anyone wanting to access server **B** from the Internet must use port 8100.

Figure 173 Port Translation Example



16.6 Port Forwarding Screen

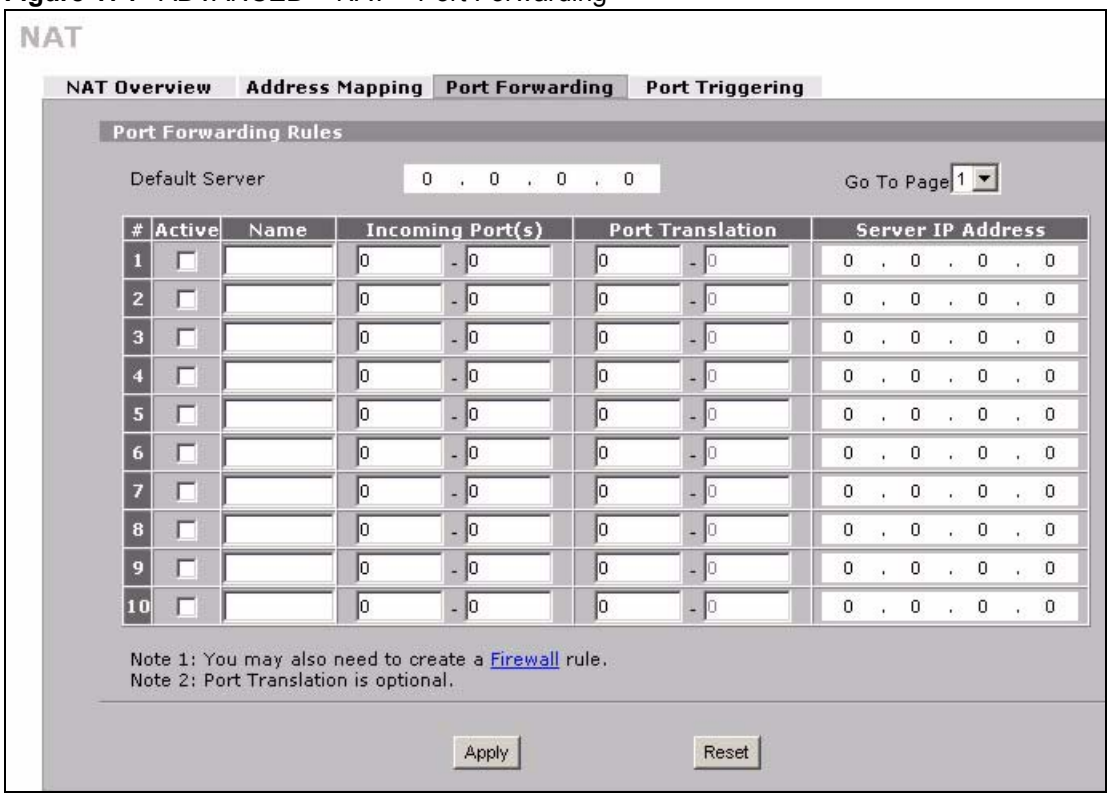
Click **ADVANCED** > **NAT** > **Port Forwarding** to open the **Port Forwarding** screen.

If you do not assign a default server IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

Refer to Appendix D on page 463 for port numbers commonly used for particular services.

The last port forwarding rule is reserved for Roadrunner services. The rule is activated only when you set the WAN encapsulation to Ethernet and the **Service Type** to something other than **Standard**.

Figure 174 ADVANCED > NAT > Port Forwarding


NAT
NAT Overview
Address Mapping
Port Forwarding
Port Triggering
Port Forwarding Rules
Default Server
0 . 0 . 0 . 0
Go To Page 1
Active Name Incoming Port(s) Port Translation Server IP Address
1 2 3 4 5 6 7 8 9 10
Note 1: You may also need to create a Firewall rule.
Note 2: Port Translation is optional.
Apply
Reset

The following table describes the labels in this screen.

Table 91 ADVANCED > NAT > Port Forwarding

LABEL	DESCRIPTION
WAN Interface	Select the WAN port for which you want to view or configure address mapping rules.
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a **Default Server** IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.
Go To Page	Choose a page from the drop-down list box to display the corresponding summary page of the port forwarding servers.
#	This is the number of an individual port forwarding server entry.
Active	Select this check box to enable the port forwarding server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule.
Incoming Port(s)	Enter a port number here. To forward only one port, enter it again in the second field. To specify a range of ports, enter the last port to be forwarded in the second field.
Port Translation	Enter the port number here to which you want the ZyWALL to translate the incoming port. For a range of ports, you only need to enter the first number of the range to which you want the incoming ports translated, the ZyWALL automatically calculates the last port of the translated port range.
Server IP Address	Enter the inside IP address of the server here.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

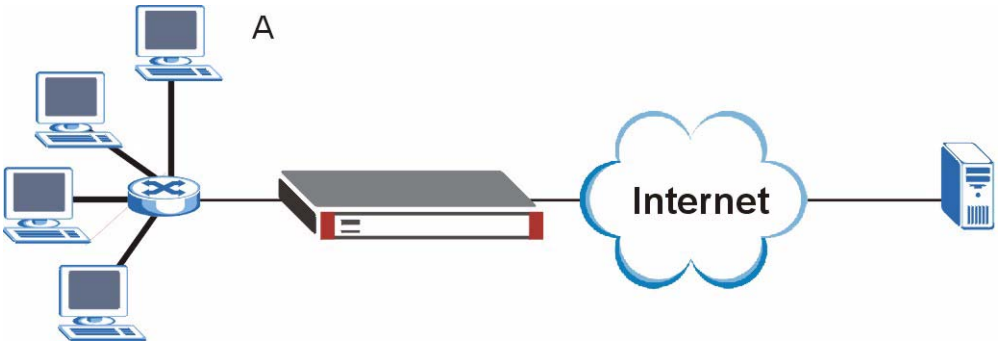
16.7 Port Triggering

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyWALL records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyWALL's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyWALL forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

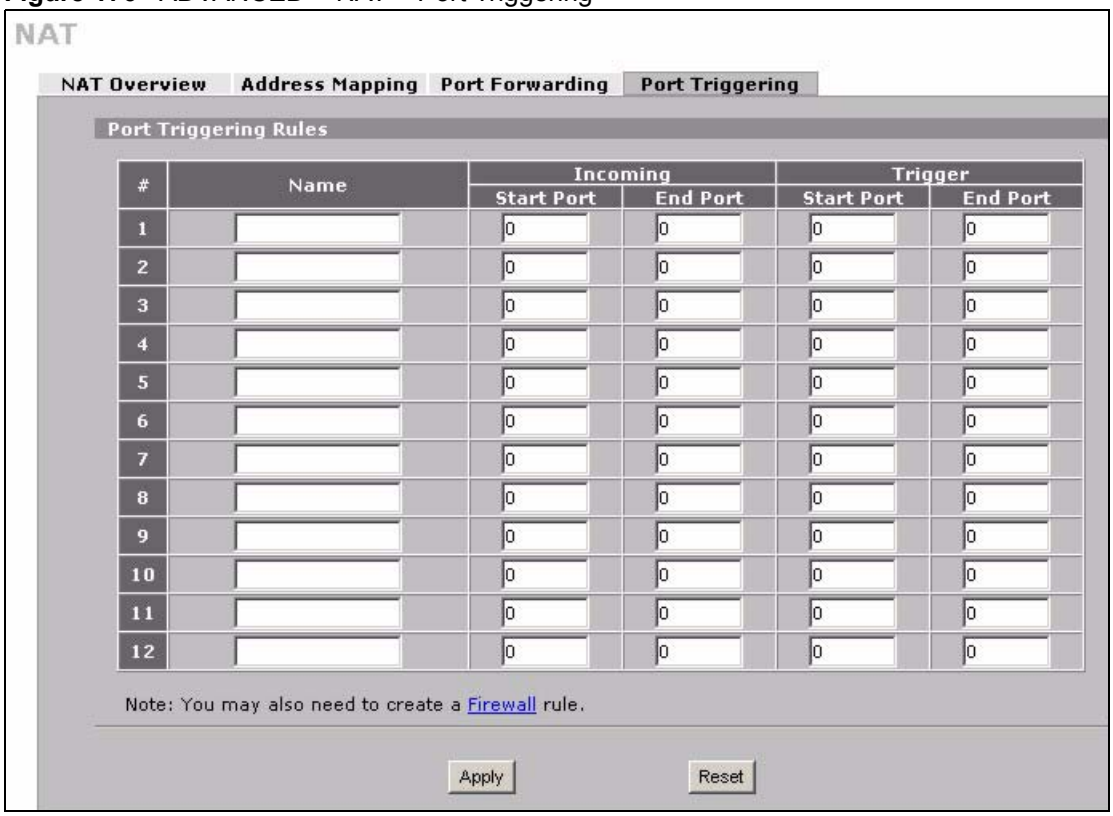
Figure 175 Trigger Port Forwarding Process: Example



1. Jane (A) requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the ZyWALL to record Jane's computer IP address. The ZyWALL associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The ZyWALL forwards the traffic to Jane's computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyWALL times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **ADVANCED** > **NAT** > **Port Triggering** to open the following screen. Use this screen to change your ZyWALL's trigger port settings.

Figure 176 ADVANCED > NAT > Port Triggering



The following table describes the labels in this screen.

Table 92 ADVANCED > NAT > Port Triggering

LABEL	DESCRIPTION
WAN Interface	Select the WAN port for which you want to view or configure address mapping rules.
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyWALL forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyWALL to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

17

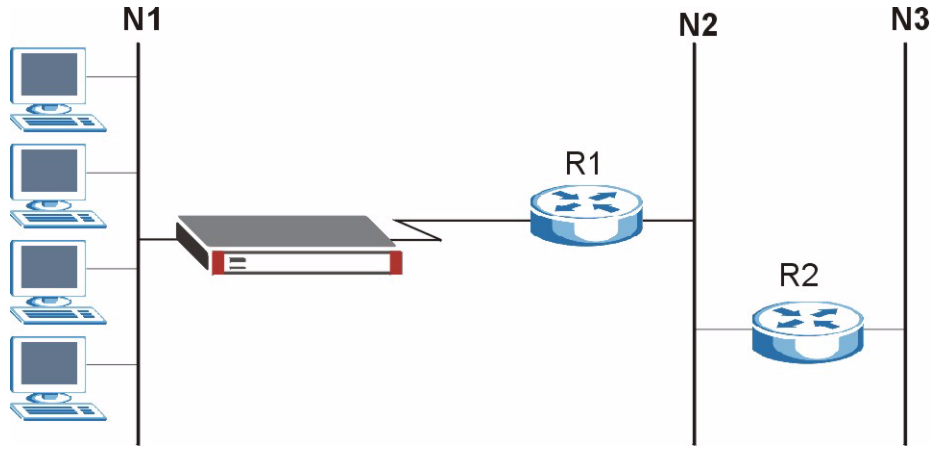
Static Route

This chapter shows you how to configure static routes for your ZyWALL.

17.1 IP Static Route

Each remote node specifies only the network to which the gateway is directly connected, and the ZyWALL has no knowledge of the networks beyond. For instance, the ZyWALL knows about network N2 in the following figure through remote node Router 1. However, the ZyWALL is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyWALL about the networks beyond the remote nodes.

Figure 177 Example of Static Routing Topology



17.2 IP Static Route

Click **ADVANCED** > **STATIC ROUTE** to open the **IP Static Route** screen (some of the screen's blank rows are not shown).

The first static route entry is for the default WAN route. You cannot modify or delete a static default route.

The default route is disabled after you change the static WAN IP address to a dynamic WAN IP address.

Figure 178 ADVANCED > STATIC ROUTE > IP Static Route

The following table describes the labels in this screen.

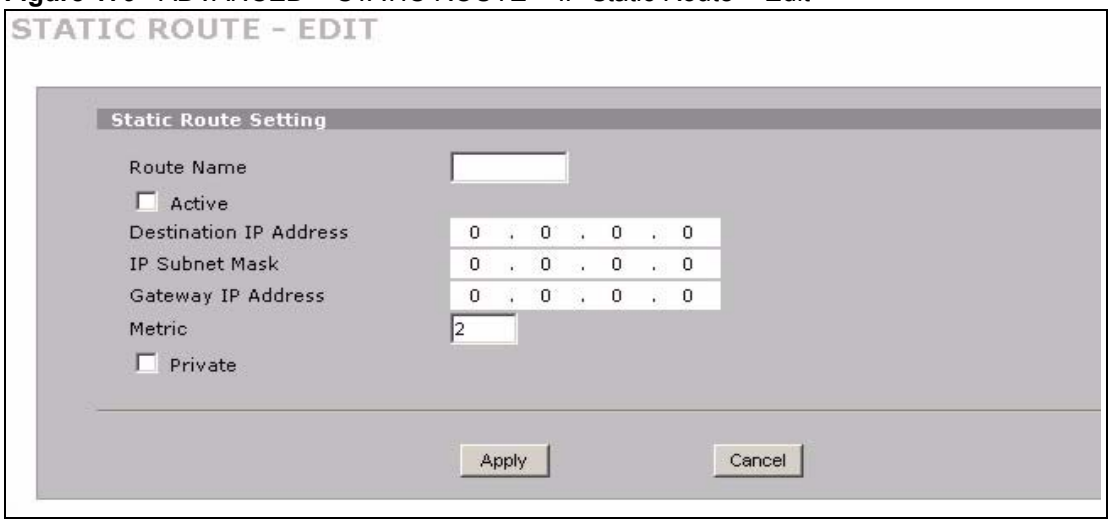
Table 93 ADVANCED > STATIC ROUTE > IP Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Name	This is the name that describes or identifies this route.
Active	This field shows whether this static route is active (**Yes**) or not (**No**).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the ZyWALL's interface. The gateway helps forward packets to their destinations.
Modify	Click the edit icon to go to the screen where you can set up a static route on the ZyWALL. Click the delete icon to remove a static route from the ZyWALL. A window displays asking you to confirm that you want to delete the route.

17.2.1 IP Static Route Edit

Select a static route index number and click **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 179 ADVANCED > STATIC ROUTE > IP Static Route > Edit



The following table describes the labels in this screen.

Table 94 ADVANCED > STATIC ROUTE > IP Static Route > Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Use the metric to set the priority of the static route. If packets match more than one static route, the ZyWALL sends them out through the route with the lowest metric. Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyWALL will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

18

Remote Management

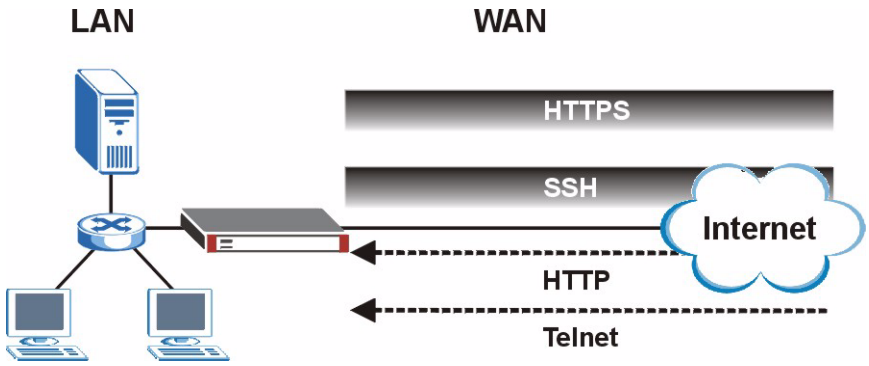
This chapter provides information on the **Remote Management** screens.

18.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyWALL interface (if any) from which computers.

The following figure shows secure and insecure management of the ZyWALL coming in from the WAN. HTTPS and SSH access are secure. HTTP and Telnet access are not secure.

Figure 180 Secure and Insecure Remote Management From the WAN



When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See Chapter 9 on page 141 for details on configuring firewall rules.

You can disable a service on the ZyWALL by not allowing access for the service/protocol through any of the ZyWALL interfaces.

You may only have one remote management session running at a time. The ZyWALL automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. SSH
2. Telnet

3 HTTPS and HTTP

18.1.1 Remote Management Limitations

Remote management does not work when:

1. You have not enabled that service on the interface in the corresponding remote management screen.
2. The IP address in the **Secure Client IP Address** field does not match the client IP address. If it does not match, the ZyWALL disconnects the session immediately.
3. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
4. There is a firewall rule that blocks it.
5. A filter is applied (through the commands) to block a Telnet, FTP or Web service.

18.1.2 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyWALL automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **MAINTENANCE** > **General** screen (see Section 24.3 on page 375).

18.2 WWW (HTTP and HTTPS)

You can set the ZyWALL to use HTTP or HTTPS (HTTPS adds security) for web configurator sessions. Specify which interfaces allow web configurator access and from which IP address the access can come.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys (see Chapter 14 on page 243 for more information).

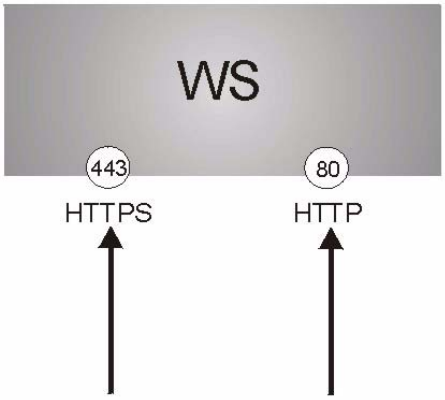
HTTPS on the ZyWALL is used so that you may securely access the ZyWALL using the web configurator. The SSL protocol specifies that the SSL server (the ZyWALL) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL), whereas the SSL client only should authenticate itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT > WWW** screen). **Authenticate Client Certificates** is optional and if selected means the SSL-client must send the ZyWALL a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyWALL.

Please refer to the following figure.

1. HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyWALL's WS (web server).

2 HTTP connection requests from a web browser go to port 80 (by default) on the ZyWALL's WS (web server).

Figure 181 HTTPS Implementation

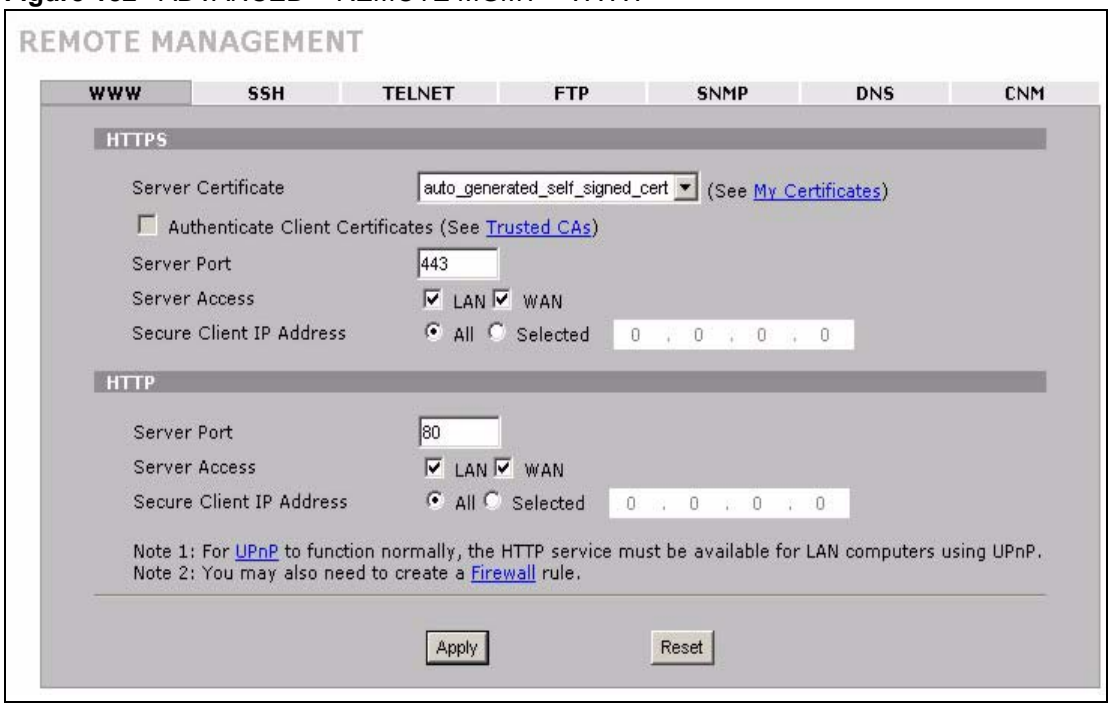


If you disable the HTTP service in the **REMOTE MGMT > WWW** screen, then the ZyWALL blocks all HTTP connection attempts.

18.3 WWW Configuration

Click **ADVANCED** > **REMOTE MGMT** to open the **WWW** screen.

Figure 182 ADVANCED > REMOTE MGMT > WWW



The following table describes the labels in this screen.

Table 95 ADVANCED > REMOTE MGMT > WWW

LABEL	DESCRIPTION
HTTPS	
Server Certificate	Select the **Server Certificate** that the ZyWALL will use to identify itself. The ZyWALL is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL).
Authenticate Client Certificates	Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the ZyWALL by sending the ZyWALL a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyWALL (see Appendix F on page 471 on importing certificates for details).
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the ZyWALL, for example 8443, then you must notify people who need to access the ZyWALL web configurator to use “https://ZyWALL IP Address:**8443**” as the URL.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service. You can allow only secure web configurator access by clearing all of the interface check boxes in the **HTTP Server Access** field and selecting interfaces in the **HTTPS Server Access** field.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service. Select **All** to allow any computer to access the ZyWALL using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
HTTP	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

Table 95 ADVANCED > REMOTE MGMT > WWW (continued)

LABEL	DESCRIPTION
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service. Select **All** to allow any computer to access the ZyWALL using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

18.4 HTTPS Example

If you have not changed the default HTTPS port on the ZyWALL, then in your browser enter “https://ZyWALL IP Address/” as the web site address where “ZyWALL IP Address” is the IP address or domain name of the ZyWALL you wish to access.

18.4.1 Internet Explorer Warning Messages

When you attempt to access the ZyWALL HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the ZyWALL.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 183 Security Alert Dialog Box (Internet Explorer)

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

18.4.2 Netscape Navigator Warning Messages

When you attempt to access the ZyWALL HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the ZyWALL.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the ZyWALL's certificate into the SSL client.

Figure 184 Security Certificate 1 (Netscape)

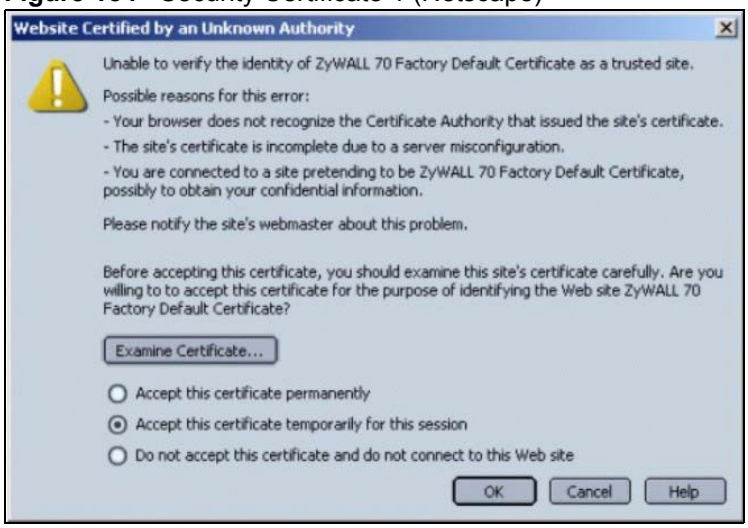

Website Certified by an Unknown Authority
Unable to verify the identity of ZyWALL 70 Factory Default Certificate as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be ZyWALL 70 Factory Default Certificate, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site ZyWALL 70 Factory Default Certificate?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
OK
Cancel
Help

Figure 185 Security Certificate 2 (Netscape)

Security Error: Domain Name Mismatch
You have attempted to establish a connection with "192.168.1.1". However, the security certificate presented belongs to "ZyWALL 70 Factory Default Certificate". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.
If you suspect the certificate shown does not belong to "192.168.1.1", please cancel the connection and notify the site administrator.
View Certificate
OK
Cancel
Help

18.4.3 Avoiding the Browser Warning Messages

The following describes the main reasons that your browser displays warnings about the ZyWALL's HTTPS server certificate and what you can do to avoid seeing the warnings.

- The issuing certificate authority of the ZyWALL's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the ZyWALL's factory default certificate is the ZyWALL itself since the certificate is a self-signed certificate.
  - For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.

- To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to Appendix F on page 471 for details.

- The actual IP address of the HTTPS server (the IP address of the ZyWALL's port that you are trying to access) does not match the common name specified in the ZyWALL's HTTPS server certificate that your browser received. Do the following to check the common name specified in the certificate that your ZyWALL sends to HTTPS clients.

  2a Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.

  2b Click **CERTIFICATES**. Find the certificate and check its **Subject** column. **CN** stands for certificate's common name (see Figure 188 on page 304 for an example).

Use this procedure to have the ZyWALL use a certificate with a common name that matches the ZyWALL's actual IP address. You cannot use this procedure if you need to access the WAN port and it uses a dynamically assigned IP address.

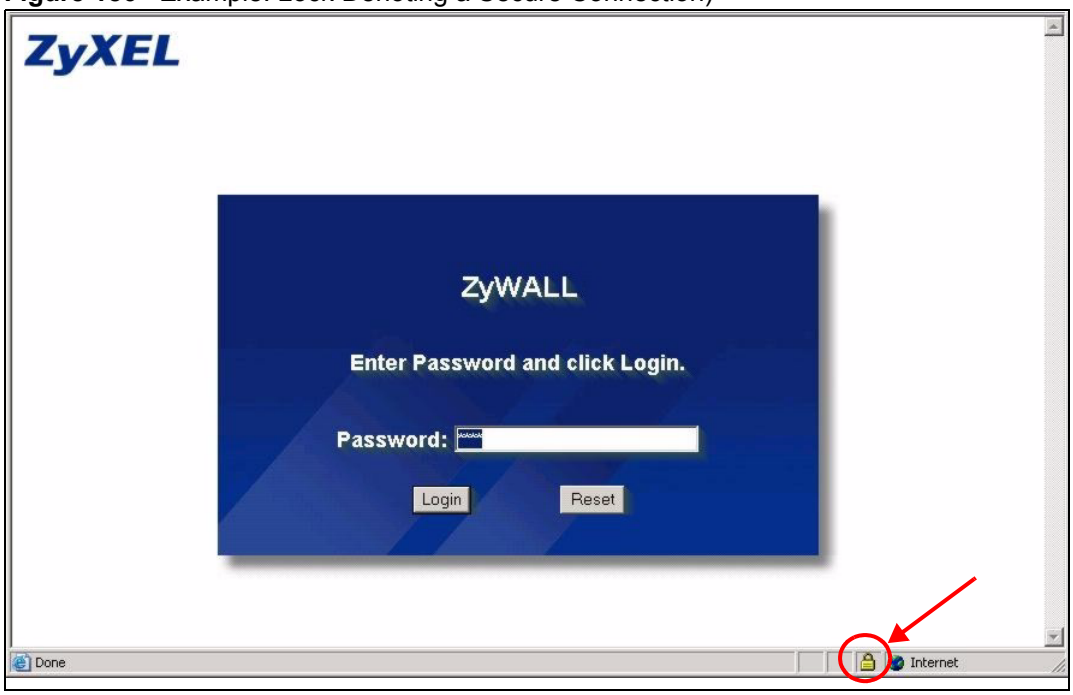
2a Create a new certificate for the ZyWALL that uses the IP address (of the ZyWALL's port that you are trying to access) as the certificate's common name. For example, to use HTTPS to access a LAN port with IP address 192.168.167.1, create a certificate that uses 192.168.167.1 as the common name.

2b Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

18.4.4 Login Screen

After you accept the certificate, the ZyWALL login screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

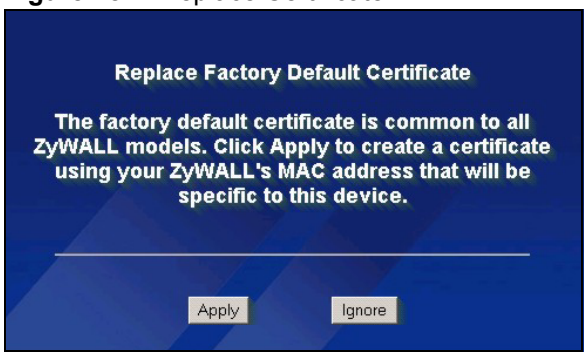
Figure 186 Example: Lock Denoting a Secure Connection)



Click **Login** and you then see the next screen.

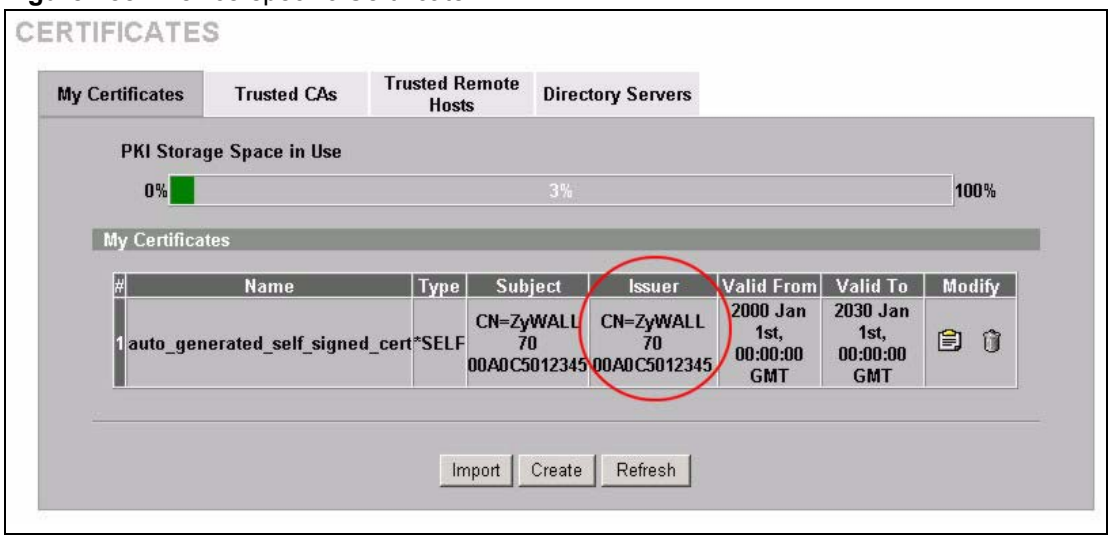
The factory default certificate is a common default certificate for all ZyWALL models.

Figure 187 Replace Certificate


Replace Factory Default Certificate
The factory default certificate is common to all ZyWALL models. Click Apply to create a certificate using your ZyWALL's MAC address that will be specific to this device.
Apply
Ignore

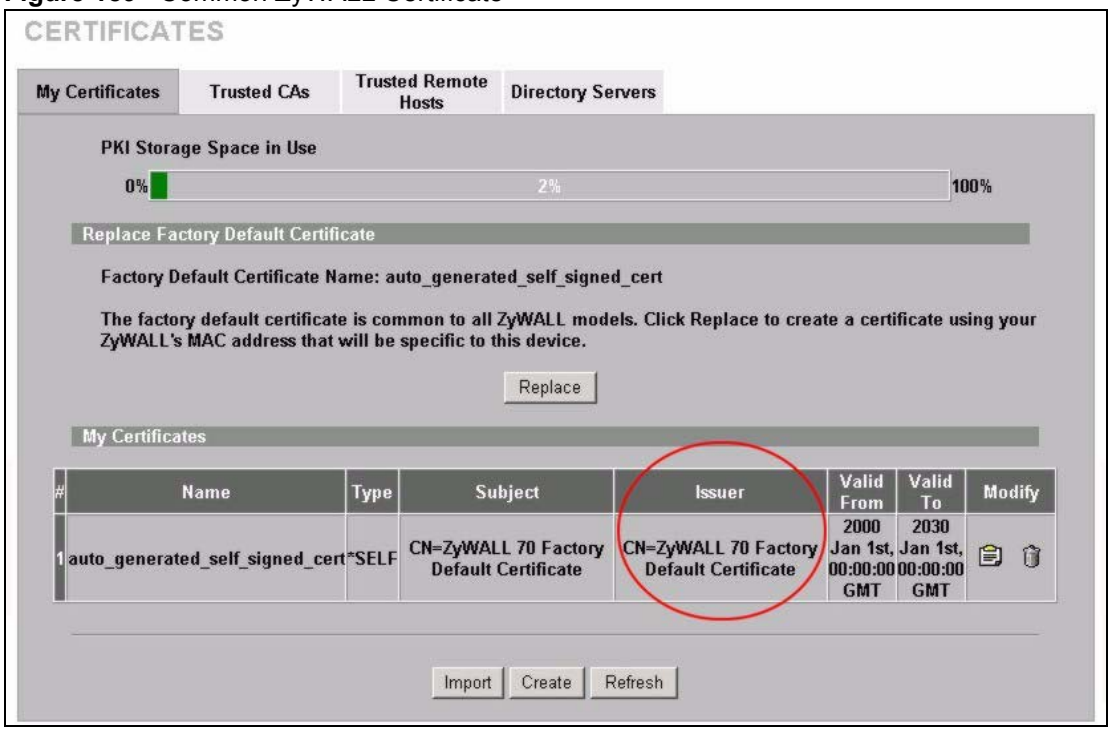
Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyWALL's MAC address that will be specific to this device. Click **CERTIFICATES** to open the **My Certificates** screen. You will see information similar to that shown in the following figure.

Figure 188 Device-specific Certificate



Click **Ignore** in the **Replace Certificate** screen to use the common ZyWALL certificate. You will then see this information in the **My Certificates** screen.

Figure 189 Common ZyWALL Certificate

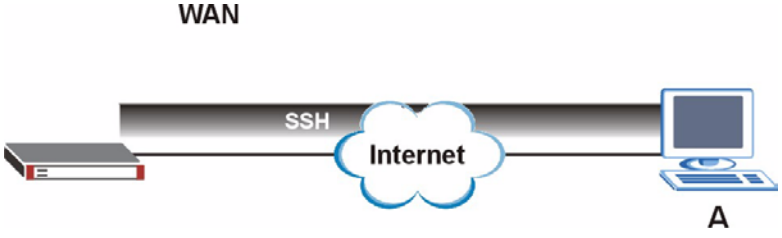

CERTIFICATES
My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers
PKI Storage Space in Use
0%
2%
100%
Replace Factory Default Certificate
Factory Default Certificate Name: auto_generated_self_signed_cert
The factory default certificate is common to all ZyWALL models. Click Replace to create a certificate using your ZyWALL's MAC address that will be specific to this device.
Replace
My Certificates
Name Type Subject Issuer Valid From Valid To Modify
1 auto_generated_self_signed_cert *SELF CN=ZyWALL 70 Factory Default Certificate CN=ZyWALL 70 Factory Default Certificate 2000 Jan 1st, 00:00:00 GMT 2030 Jan 1st, 00:00:00 GMT
Import
Create
Refresh

18.5 SSH

You can use SSH (Secure SHell) to securely access the ZyWALL's command line interface. Specify which interfaces allow SSH access and from which IP address the access can come.

Unlike Telnet or FTP, which transmit data in plaintext (clear or unencrypted text), SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer **A** on the Internet uses SSH to securely connect to the WAN port of the ZyWALL for a management session.

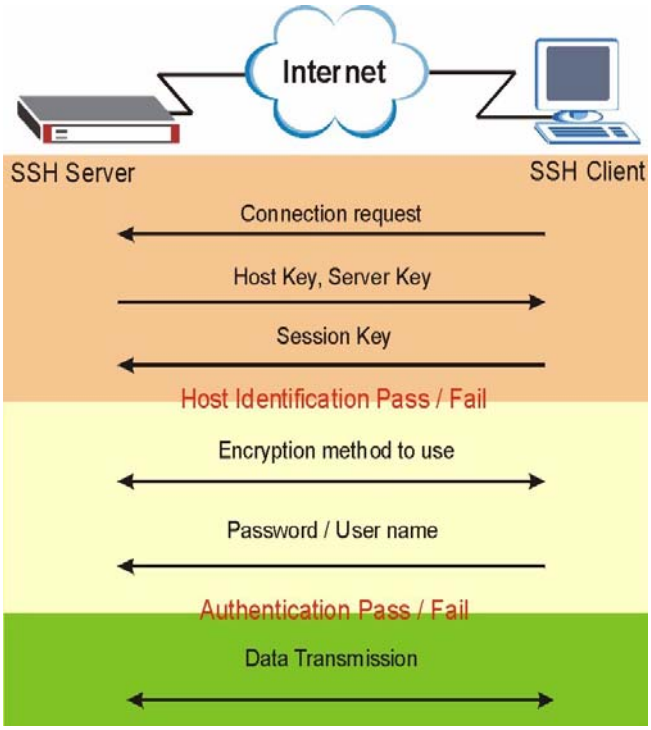
Figure 190 SSH Communication Over the WAN Example



18.6 How SSH Works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 191 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

18.7 SSH Implementation on the ZyWALL

Your ZyWALL supports SSH version 1.5 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the ZyWALL for remote command line interface access and file transfer on port 22. Only one SSH connection is allowed at a time.

18.7.1 Requirements for Using SSH

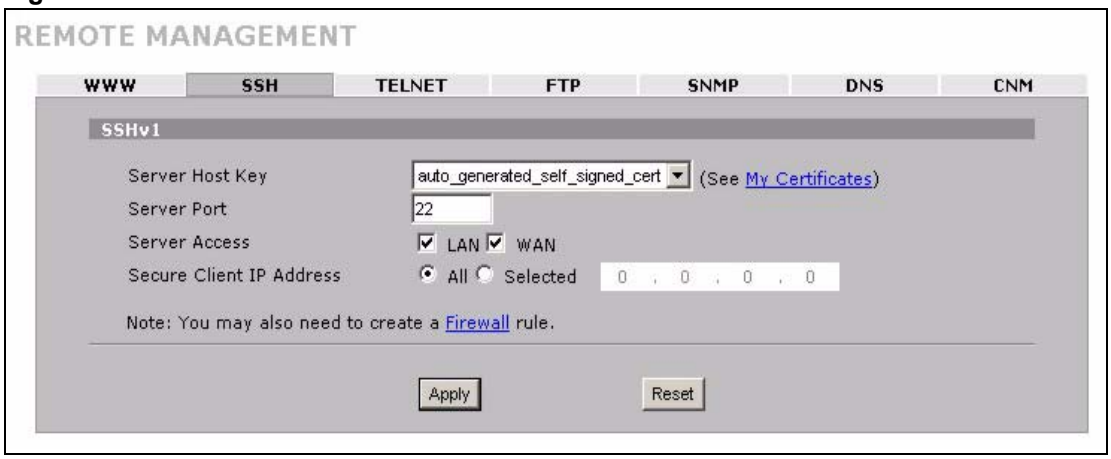
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyWALL over SSH.

18.8 Configuring SSH

Click **ADVANCED** > **REMOTE MGMT** > **SSH** to change your ZyWALL's Secure Shell settings.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 192 ADVANCED > REMOTE MGMT > SSH



The following table describes the labels in this screen.

Table 96 ADVANCED > REMOTE MGMT > SSH

LABEL	DESCRIPTION
Server Host Key	Select the certificate whose corresponding private key is to be used to identify the ZyWALL for SSH connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 14 on page 243 for details).
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service. Clear all of the interface check boxes to disable SSH access to the ZyWALL.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service. Select **All** to allow any computer to access the ZyWALL using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

18.9 Secure Telnet Using SSH Examples

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the ZyWALL. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

18.9.1 Example 1: Microsoft Windows

This section describes how to access the ZyWALL using the Secure Shell Client program.

1. Launch the SSH client and specify the connection information (IP address, port number or device name) for the ZyWALL.
2. Configure the SSH client to accept connection using SSH version 1.
3. A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 193 SSH Example 1: Store Host Key

Host Identification
You are connecting to the host "192.168.1.1" for the first time.
The host has provided you its identification, a host public key.
The fingerprint of the host public key is:
"xevac-bycor-kubyz-dipah-ravut-fyduz-kazuk-goler-cavom-hifot-sexox"
You can save the host key to the local database by clicking Yes.
You can continue without saving the host key by clicking No.
You can also cancel the connection by clicking Cancel.
Do you want to save the new host key to the local database?
Yes
No
Cancel
Help

Enter the password to log in to the ZyWALL. The command line interface displays next.

18.9.2 Example 2: Linux

This section describes how to access the ZyWALL using the OpenSSH client program that comes with most Linux distributions.

1. Test whether the SSH service is available on the ZyWALL.

   Enter "`telnet 192.168.167.1 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the ZyWALL (using the default IP address of 192.168.167.1).

   A message displays indicating the SSH protocol version supported by the ZyWALL.

Figure 194 SSH Example 2: Test

```
$ telnet 192.168.167.1 22
Trying 192.168.167.1...
Connected to 192.168.167.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter "ssh -1 192.168.167.1". This command forces your computer to connect to the ZyWALL using SSH version 1. If this is the first time you are connecting to the ZyWALL using SSH, a message displays prompting you to save the host information of the ZyWALL. Type "yes" and press [ENTER].

Then enter the password to log in to the ZyWALL.

Figure 195 SSH Example 2: Log in

```
$ ssh -1 192.168.167.1
The authenticity of host '192.168.167.1 (192.168.167.1)' can't be
established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.167.1' (RSA1) to the list of known
hosts.
Administrator@192.168.167.1's password:
```

3 The command line interface displays next.

18.10 Secure FTP Using SSH Example

This section shows an example on file transfer using the OpenSSH client program. The configuration and connection steps are similar for other SSH client programs. Refer to your SSH client program user's guide.

1 Enter "sftp -1 192.168.167.1". This command forces your computer to connect to the ZyWALL for secure file transfer using SSH version 1. If this is the first time you are connecting to the ZyWALL using SSH, a message displays prompting you to save the host information of the ZyWALL. Type "yes" and press [ENTER].

2 Enter the password to login to the ZyWALL.

3 Use the "put" command to upload a new firmware to the ZyWALL.

Figure 196 Secure FTP: Firmware Upload Example

```
$ sftp -1 192.168.167.1
Connecting to 192.168.167.1...
The authenticity of host '192.168.167.1 (192.168.167.1)' can't be
established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.167.1' (RSA1) to the list of known
hosts.
Administrator@192.168.167.1's password:
sftp> put firmware.bin ras
Uploading firmware.bin to /ras
Read from remote host 192.168.167.1: Connection reset by peer
Connection closed
$
```

18.11 Telnet

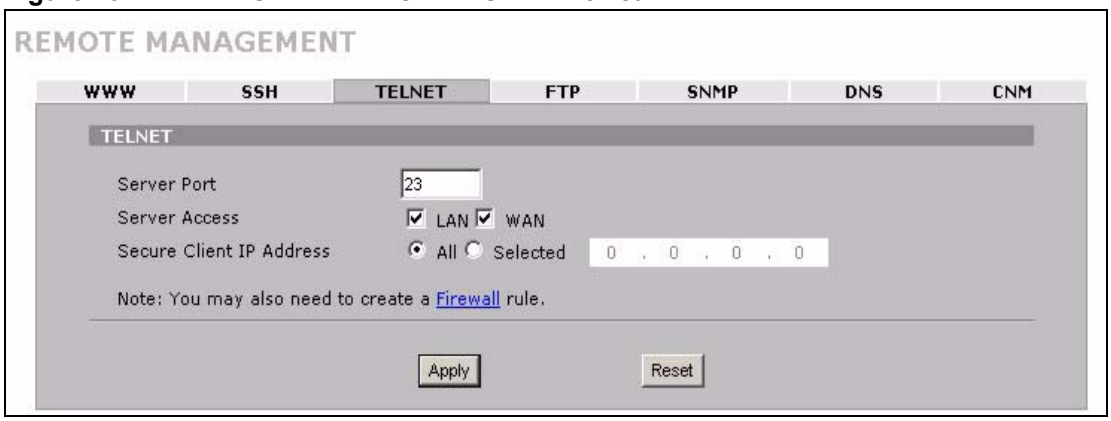
You can use Telnet to access the ZyWALL's command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

18.12 Configuring TELNET

Click **ADVANCED** > **REMOTE MGMT** > **TELNET** to open the following screen. Use this screen to specify which interfaces allow Telnet access and from which IP address the access can come.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 197 ADVANCED > REMOTE MGMT > Telnet



The following table describes the labels in this screen.

Table 97 ADVANCED > REMOTE MGMT > Telnet

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service. Clear all of the interface check boxes to disable Telnet access to the ZyWALL.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service. Select **All** to allow any computer to access the ZyWALL using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

18.13 Telnet Login

Use the following steps to Telnet into your ZyWALL's command interpreter. See Appendix G on page 481 for more about the commands.

1. If your computer is connected to the ZyWALL over the Internet, skip to the next step. Make sure your computer IP address and the ZyWALL IP address are on the same subnet.
2. In Windows, click **Start** (usually in the bottom left corner) and **Run**. Then type `telnet` and the ZyWALL's IP address. For example, enter `telnet 192.168.167.1` (the default IP address).
3. Click **OK**. A login screen displays. Enter the password at the prompts.

The default password is **1234**. The password is case-sensitive.

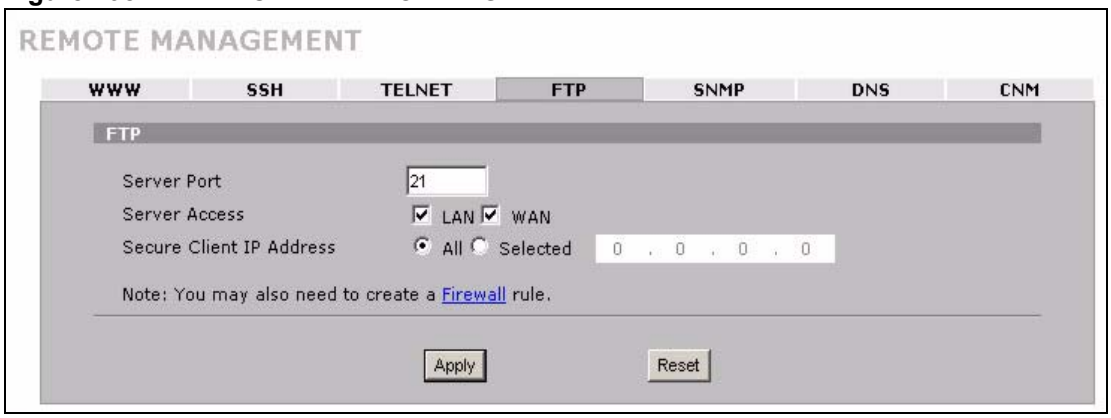
18.14 FTP

You can use FTP (File Transfer Protocol) to upload and download the ZyWALL's firmware and configuration files, please see the user's guide Chapter 24 on page 375 for details. To use this feature, your computer must have an FTP client.

To change your ZyWALL's FTP settings, click **ADVANCED** > **REMOTE MGMT** > **FTP**. The screen appears as shown. Use this screen to specify which interfaces allow FTP access and from which IP address the access can come.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

Figure 198 ADVANCED > REMOTE MGMT > FTP



The following table describes the labels in this screen.

Table 98 ADVANCED > REMOTE MGMT > FTP

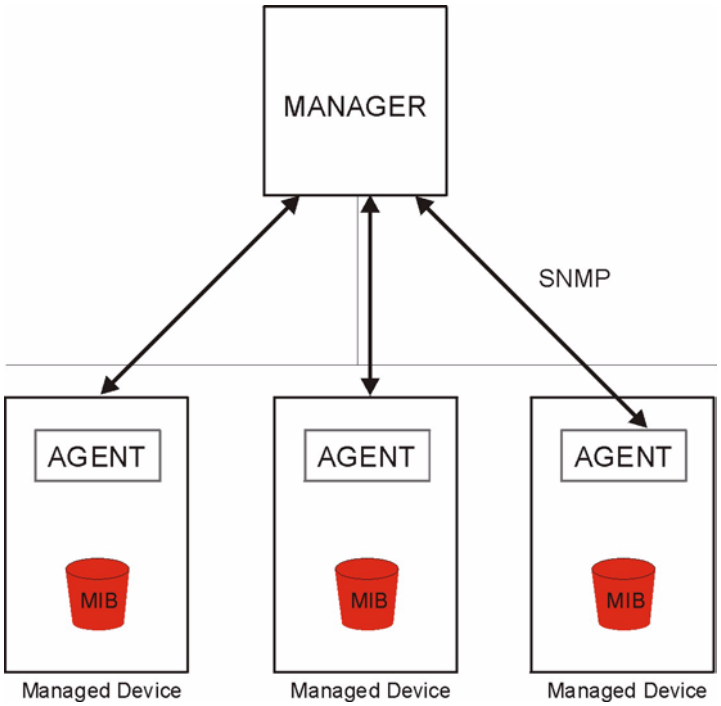
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service. Clear all of the interface check boxes to disable FTP access to the ZyWALL.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service. Select **All** to allow any computer to access the ZyWALL using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

18.15 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

SNMP is only available if TCP/IP is configured.

Figure 199 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyWALL). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

18.15.1 Supported MIBs

The ZyWALL supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

18.15.2 SNMP Traps

The ZyWALL sends traps to the SNMP manager when one of the following events occurs:

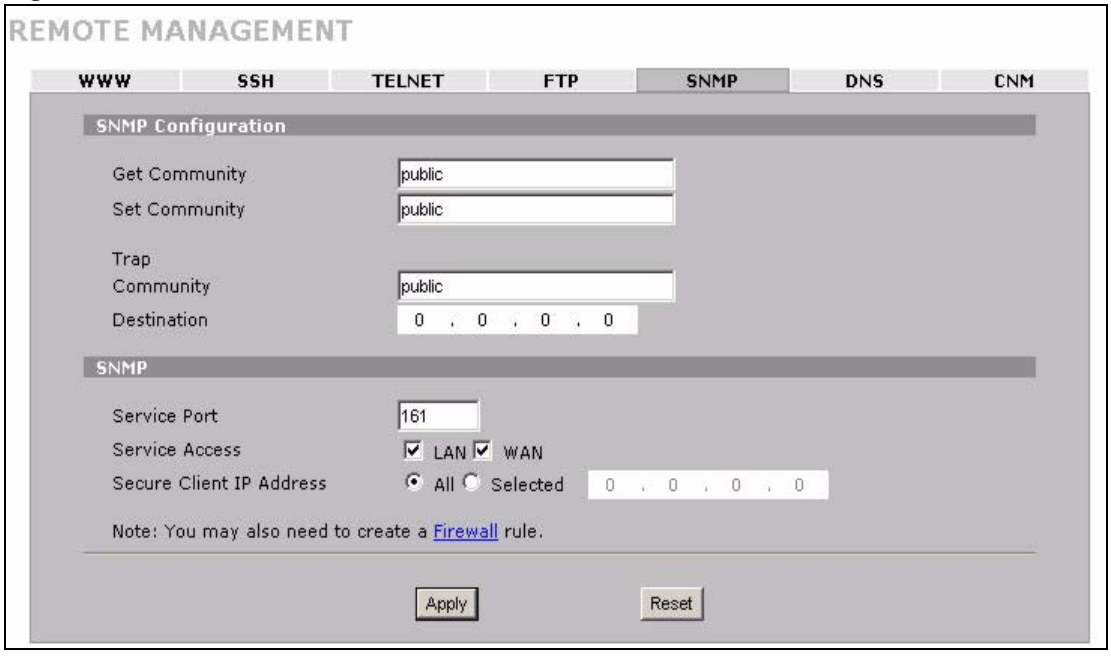
Table 99 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

18.15.3 REMOTE MANAGEMENT: SNMP

To change your ZyWALL's SNMP settings, click **ADVANCED** > **REMOTE MGMT** > **SNMP**. The screen appears as shown.

Figure 200 ADVANCED > REMOTE MGMT > SNMP



The following table describes the labels in this screen.

Table 100 ADVANCED > REMOTE MGMT > SNMP

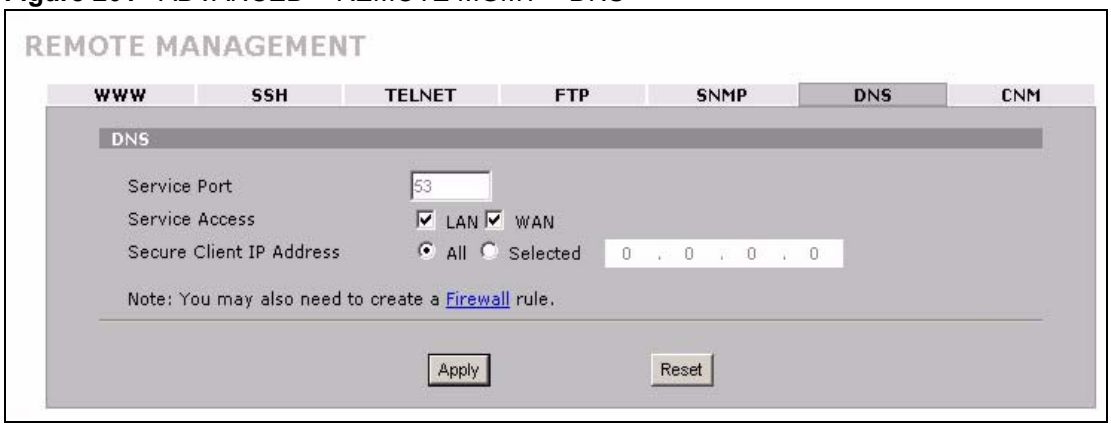
LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the ZyWALL using this service. Clear all of the interface check boxes to disable SNMP access to the ZyWALL.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service. Select **All** to allow any computer to access the ZyWALL using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

18.16 DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. Refer to Chapter 6 on page 109 for more information.

Click **ADVANCED** > **REMOTE MGMT** > **DNS** to change your ZyWALL’s DNS settings. Use this screen to set from which IP address the ZyWALL will accept DNS queries and on which interface it can send them your ZyWALL’s DNS settings. This feature is not available when the ZyWALL is set to bridge mode.

Figure 201 ADVANCED > REMOTE MGMT > DNS



The following table describes the labels in this screen.

Table 101 ADVANCED > REMOTE MGMT > DNS

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Service Access	Select the interface(s) through which a computer may send DNS queries to the ZyWALL. Clear all of the interface check boxes to have the ZyWALL discard all DNS queries destined for the ZyWALL itself.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to send DNS queries to the ZyWALL. Select **All** to allow any computer to send DNS queries to the ZyWALL. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the ZyWALL.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

18.17 Introducing Vantage CNM

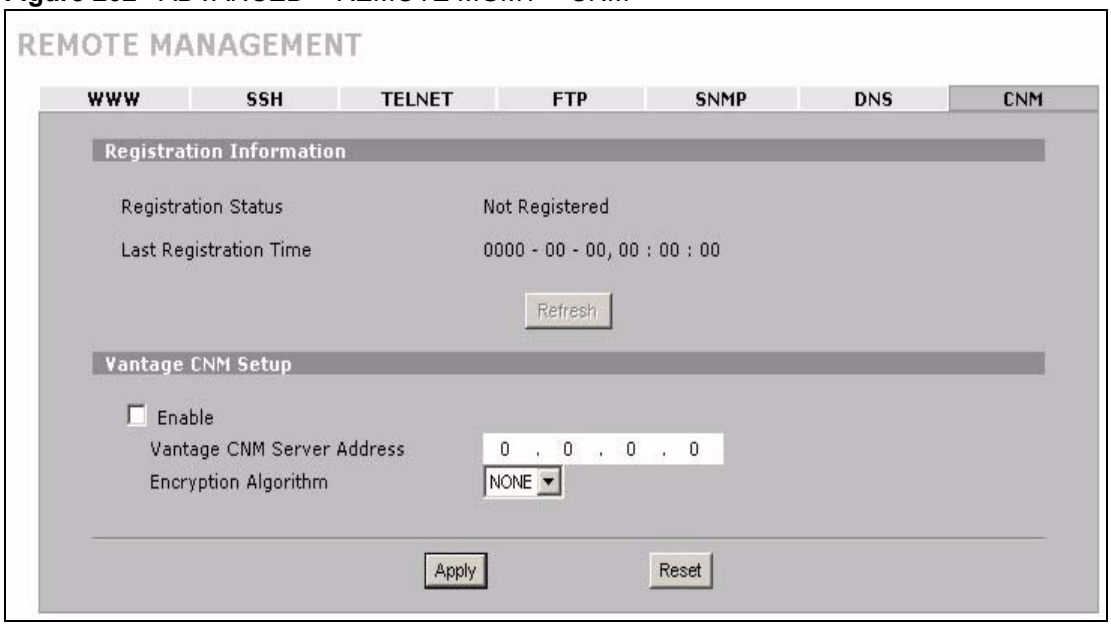
Vantage CNM (Centralized Network Management) is a browser-based global management solution that allows an administrator from any location to easily configure, manage, monitor and troubleshoot ZyXEL devices located worldwide. See the Vantage CNM User's Guide for details.

If you allow your ZyWALL to be managed by the Vantage CNM server, then you should not configure the ZyWALL (using either the web configurator or commands) without notifying the Vantage CNM administrator.

18.18 Configuring CNM

Vantage CNM is disabled on the device by default. Click **ADVANCED** > **REMOTE MGMT** > **CNM** to configure your device’s Vantage CNM settings.

Figure 202 ADVANCED > REMOTE MGMT > CNM



The following table describes the labels in this screen.

Table 102 ADVANCED > REMOTE MGMT > CNM

LABEL	DESCRIPTION
Registration Information	
Registration Status	This read only field displays **Not Registered** when **Enable** is not selected. It displays **Registering** when the ZyWALL first connects with the Vantage CNM server and then **Registered** after it has been successfully registered with the Vantage CNM server. It will continue to display **Registering** until it successfully registers with the Vantage CNM server. It will not be able to register with the Vantage CNM server if: The Vantage CNM server is down. The Vantage CNM server IP address is incorrect. The Vantage CNM server is behind a NAT router or firewall that does not forward packets through to the Vantage CNM server. The encryption algorithms and/or encryption keys do not match between the ZyWALL and the Vantage CNM server.
Last Registration Time	This field displays the last date (year-month-date) and time (hours-minutes-seconds) that the ZyWALL registered with the Vantage CNM server. It displays all zeroes if it has not yet registered with the Vantage CNM server.
Refresh	Click **Refresh** to update the registration status and last registration time.
Vantage CNM Setup	
Enable	Select this check box to allow Vantage CNM to manage your ZyWALL.
Vantage CNM Server Address	If the Vantage server is on the same subnet as the ZyXEL device, enter the private or public IP address of the Vantage server. If the Vantage CNM server is on a different subnet to the ZyWALL, enter the public IP address of the Vantage server.
Encryption Algorithm	The **Encryption Algorithm** field is used to encrypt communications between the ZyWALL and the Vantage CNM server. Choose from **None** (no encryption), **DES** or **3DES**. The **Encryption Key** field appears when you select **DES** or **3DES**. The ZyWALL must use the same encryption algorithm as the Vantage CNM server.

Table 102 ADVANCED > REMOTE MGMT > CNM (continued)

LABEL	DESCRIPTION
Encryption Key	Type eight alphanumeric characters ("0" to "9", "a" to "z" or "A" to "Z") when you choose the **DES** encryption algorithm and 24 alphanumeric characters ("0" to "9", "a" to "z" or "A" to "Z") when you choose the **3DES** encryption algorithm. The ZyWALL must use the same encryption key as the Vantage CNM server.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

18.18.1 Additional Configuration for Vantage CNM

If you have NAT routers or firewalls between the ZyWALL and the Vantage CNM server, you must configure them to forward TCP ports 8080 (HTTP), 443 (HTTPS) and 20 and 21 (FTP). They must also forward UDP ports 1864 and 1865.

19

UPnP

This chapter introduces the Universal Plug and Play feature. This chapter is only applicable when the ZyWALL is in router mode.

19.1 Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

19.1.1 How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

19.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See Chapter 16 on page 277 for further information about NAT.

19.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyWALL allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

19.1.4 UPnP and ZyXEL

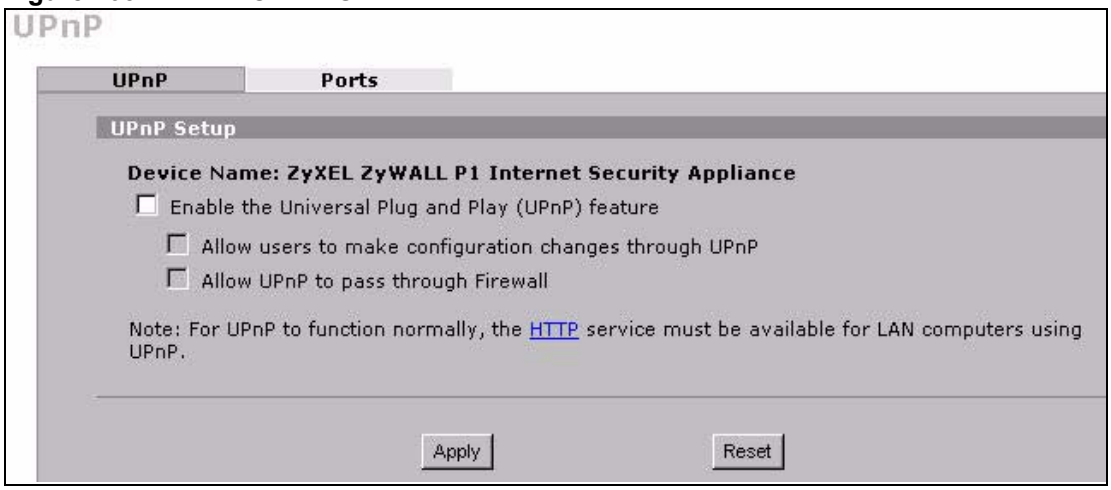
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device).

See the following sections for examples of installing and using UPnP.

19.2 Configuring UPnP

Click **ADVANCED > UPnP** to display the **UPnP** screen.

Figure 203 ADVANCED > UPnP


UPnP
UPnP
Ports
UPnP Setup
Device Name: ZyXEL ZyWALL P1 Internet Security Appliance
Enable the Universal Plug and Play (UPnP) feature
Allow users to make configuration changes through UPnP
Allow UPnP to pass through Firewall
Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
Apply
Reset

The following table describes the fields in this screen.

Table 103 ADVANCED > UPnP

LABEL	DESCRIPTION
UPnP Setup	
Device Name	This identifies the ZyXEL device in UPnP applications.
Enable the Universal Plug and Play (UPnP) feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyWALL's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyWALL so that they can communicate through the ZyWALL, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

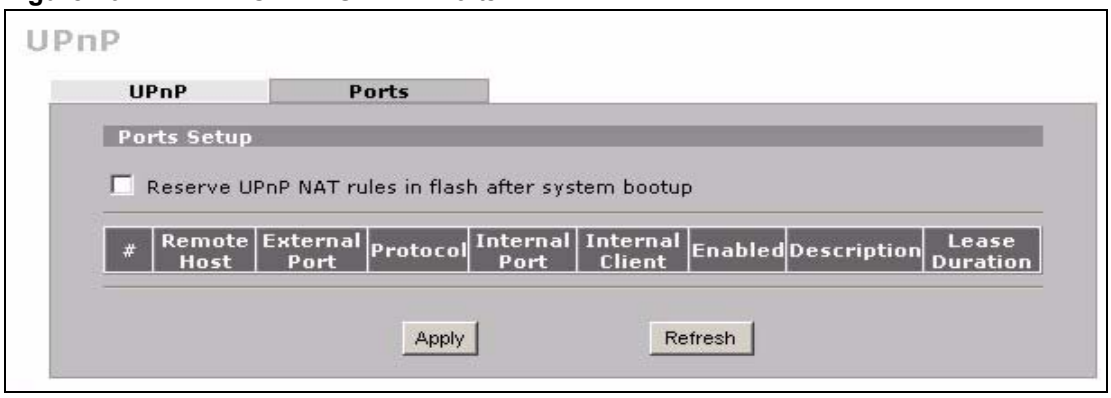
Table 103 ADVANCED > UPnP

LABEL	DESCRIPTION
Allow UPnP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Outgoing WAN Interface	Select through which WAN port you want to send out traffic from UPnP-enabled applications. If the WAN port you select loses its connection, the ZyWALL attempts to use the other WAN port. If the other WAN port also does not work, the ZyWALL drops outgoing packets from UPnP-enabled applications.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

19.3 Displaying UPnP Port Mapping

Click **ADVANCED > UPnP > Ports** to display the UPnP Ports screen. Use this screen to view the NAT port mapping rules that UPnP creates on the ZyWALL.

Figure 204 ADVANCED > UPnP > Ports



The following table describes the labels in this screen.

Table 104 ADVANCED > UPnP > Ports

LABEL	DESCRIPTION
Reserve UPnP NAT rules in flash after system bootup	Select this check box to have the ZyWALL retain UPnP created NAT rules even after restarting. If you use UPnP and you set a port on your computer to be fixed for a specific service (for example FTP for file transfers), this option allows the ZyWALL to keep a record when your computer uses UPnP to create a NAT forwarding rule for that service.
The following read-only table displays information about the UPnP-created NAT mapping rule entries in the ZyWALL's NAT routing table.	
#	This is the index number of the UPnP-created NAT mapping rule entry.
Remote Host	This field displays the source IP address (on the WAN) of inbound IP packets. Since this is often a wildcard, the field may be blank. When the field is blank, the ZyWALL forwards all traffic sent to the **External Port** on the WAN interface to the **Internal Client** on the **Internal Port**. When this field displays an external IP address, the NAT rule has the ZyWALL forward inbound packets to the **Internal Client** from that IP address only.

Table 104 ADVANCED > UPnP > Ports (continued)

LABEL	DESCRIPTION
External Port	This field displays the port number that the ZyWALL "listens" on (on the WAN port) for connection requests destined for the NAT rule's **Internal Port** and **Internal Client**. The ZyWALL forwards incoming packets (from the WAN) with this port number to the **Internal Client** on the **Internal Port** (on the LAN). If the field displays "0", the ZyWALL ignores the **Internal Port** value and forwards requests on all external port numbers (that are otherwise unmapped) to the **Internal Client**.
Protocol	This field displays the protocol of the NAT mapping rule (TCP or UDP).
Internal Port	This field displays the port number on the **Internal Client** to which the ZyWALL should forward incoming connection requests.
Internal Client	This field displays the DNS host name or IP address of a client on the LAN. Multiple NAT clients can use a single port simultaneously if the internal client field is set to 255.255.255.255 for UDP mappings.
Enabled	This field displays whether or not this UPnP-created NAT mapping rule is turned on. The UPnP-enabled device that connected to the ZyWALL and configured the UPnP-created NAT mapping rule on the ZyWALL determines whether or not the rule is enabled.
Description	This field displays a text explanation of the NAT mapping rule.
Lease Duration	This field displays a dynamic port-mapping rule's time to live (in seconds). It displays "0" if the port mapping is static.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Refresh	Click **Refresh** update the screen's table.

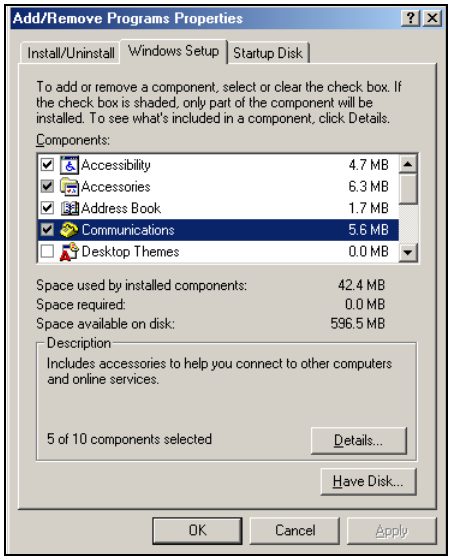
19.4 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

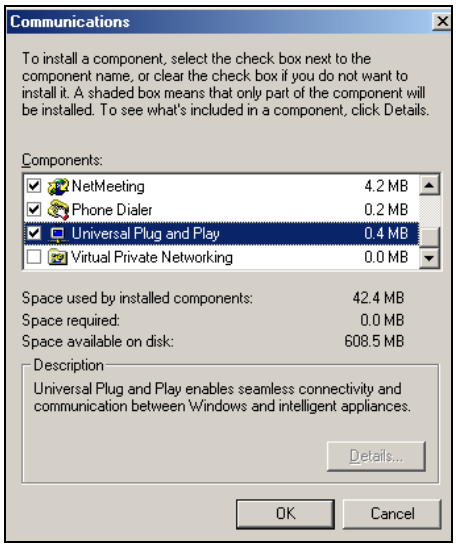
19.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

1. Click **Start**, **Settings** and **Control Panel**. Double-click **Add/Remove Programs**.
2. Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.


Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Accessibility 4.7 MB
Accessories 6.3 MB
Address Book 1.7 MB
Communications 5.6 MB
Desktop Themes 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 596.5 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 10 components selected
Details...
Have Disk...
OK
Cancel
Apply

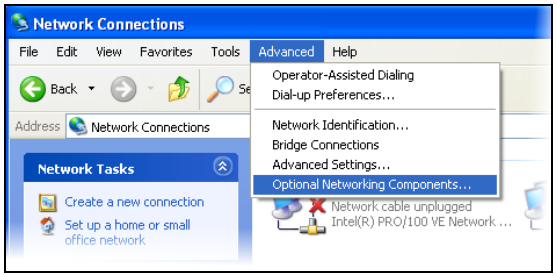
3. In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.
4. Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
5. Restart the computer when prompted.


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 608.5 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

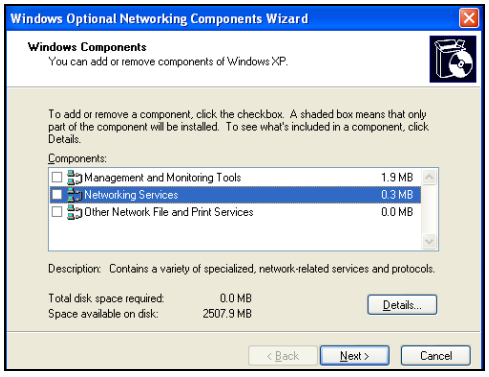
19.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

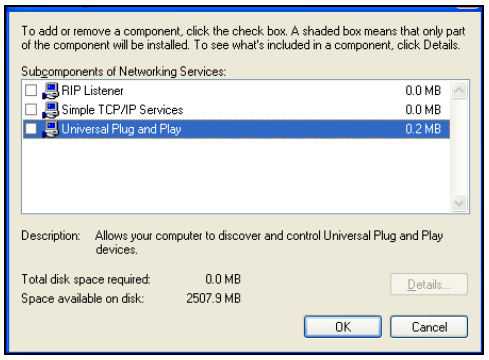
1. Click **Start**, **Settings** and **Control Panel**.
2. Double-click **Network Connections**.
3. In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components …**.
   The **Windows Optional Networking Components Wizard** window displays.



4. Select **Networking Service** in the **Components** selection box and click **Details**.


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 2507.9 MB
Details...
< Back
Next >
Cancel

5. In the **Networking Services** window, select the **Universal Plug and Play** check box.
6. Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.


To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 2507.9 MB
Details...
OK
Cancel

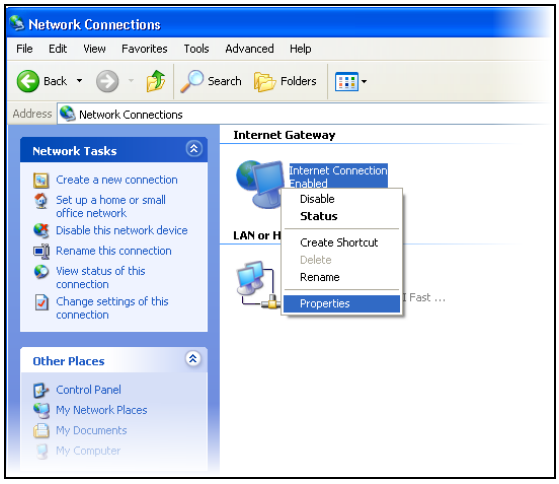
19.5 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL device.

Make sure the computer is connected to a LAN port of the ZyXEL device. Turn on your computer and the ZyXEL device.

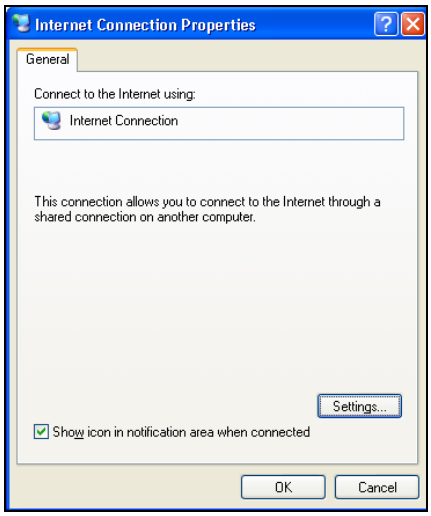
19.5.1 Auto-discover Your UPnP-enabled Network Device

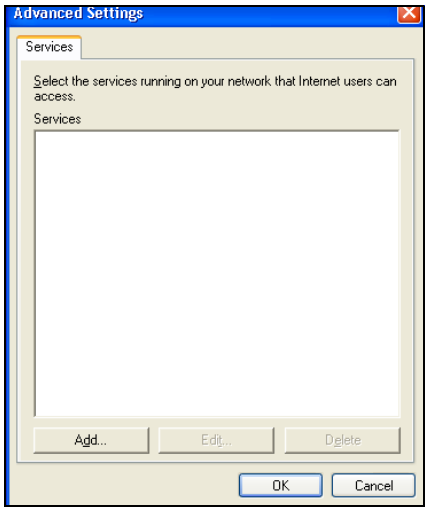
1. Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under **Internet Gateway**.
2. Right-click the icon and select **Properties**.

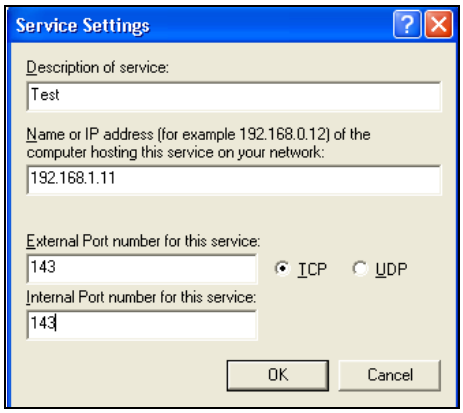


3. In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.

You may edit or delete the port mappings or click **Add** to manually add port mappings.

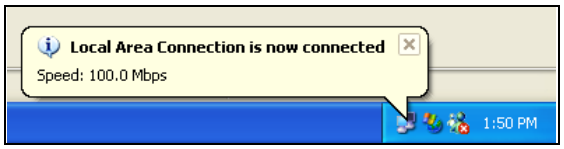

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel





When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

4 Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray.



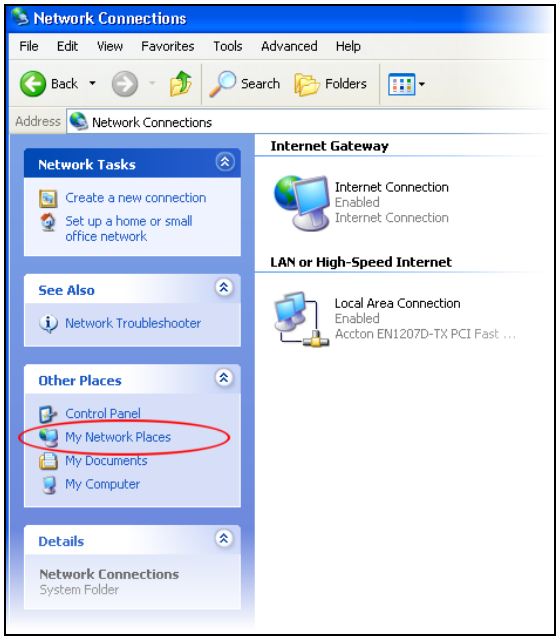
5 Double-click the icon to display your current Internet connection status.

19.5.2 Web Configurator Easy Access

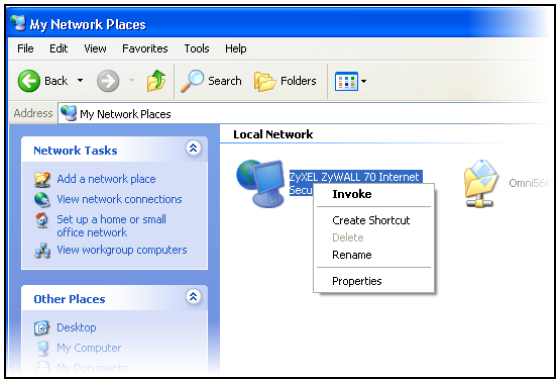
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

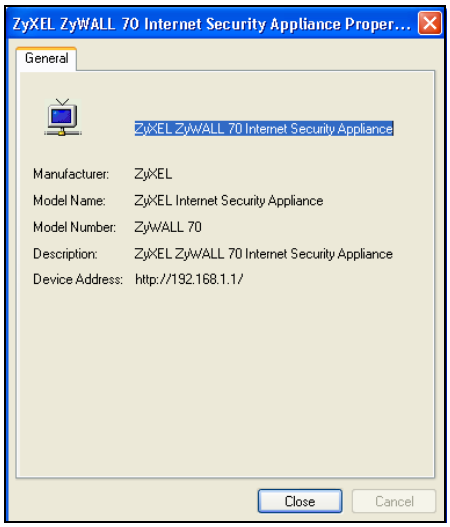
1. Click **Start** and then **Control Panel**.
2. Double-click **Network Connections**.
3. Select **My Network Places** under **Other Places**.



4. An icon with the description for each UPnP-enabled device displays under **Local Network**.
5. Right-click the icon for your ZyXEL device and select **Invoke**. The web configurator login screen displays.



6 Right-click the icon for your ZyXEL device and select **Properties**. A properties window displays with basic information about the ZyXEL device.



20

Custom Application

This chapter covers how to set the ZyWALL's to monitor custom port numbers for specific applications.

20.1 Custom Applicaton

Use custom application to have the ZyWALL's ALG, anti-virus, and content filtering features monitor traffic on custom ports, in addition to the default ports.

By default, these ZyWALL features monitor traffic for the following protocols on these port numbers.

- FTP: 21
- SIP: 5060
- H.323: 1720
- SMTP: 25
- POP3: 110
- HTTP: 80

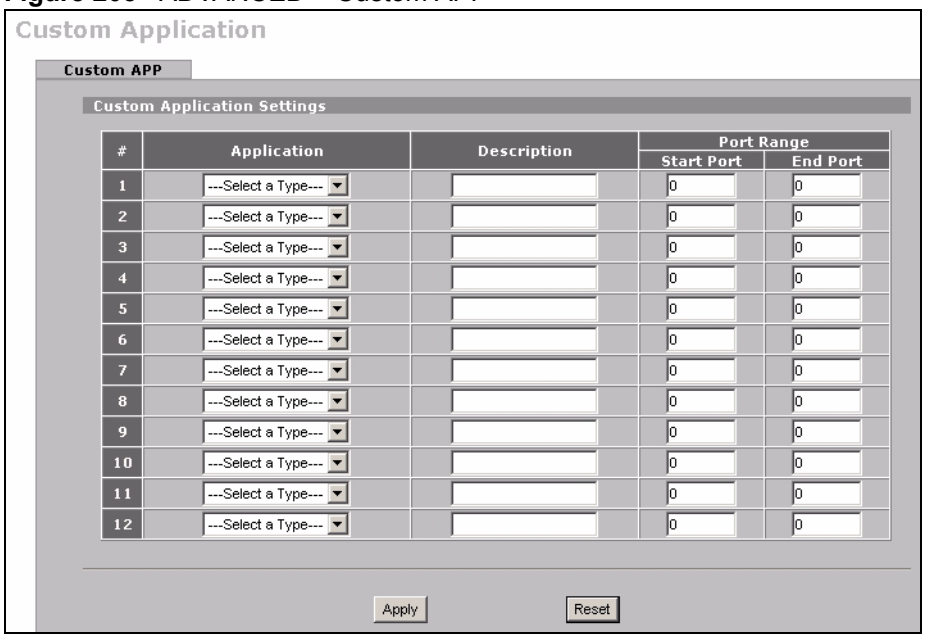
Changes in the **Custom APP** screen do not apply to the firewall.

20.2 Custom Applicaton Configuration

Click **ADVANCED > Custom APP** to open the **Custom Application** screen.

This screen only specifies what port numbers the ZyWALL checks for specific protocol traffic. Use other screens to enable or disable the monitoring of the protocol traffic.

Figure 205 ADVANCED > Custom APP



The following table describes the labels in this screen.

Table 105 ADVANCED > Custom APP

LABEL	DESCRIPTION
Application	Select the application for which you want the ZyWALL to monitor specific ports. You can use the same application in more than one entry. To remove an entry, select **Select a Type**.
Description	Enter information about the reason for monitoring custom port numbers for this protocol.
Start Port	Enter the starting port for the range that the ZyWALL is to monitor for this application. If you are only entering a single port number, enter it here.
End Port	Enter the ending port for the range that the ZyWALL is to monitor for this application.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

21

ALG Screen

This chapter covers how to use the ZyWALL's ALG feature to allow certain applications to pass through the ZyWALL.

21.1 ALG Introduction

An Application Layer Gateway (ALG) manages a specific protocol (such as SIP, H.323 or FTP) at the application layer. The ZyWALL can function as an ALG to allow certain NAT un-friendly applications (such as SIP) to operate properly through the ZyWALL.

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The ZyWALL examines and uses IP address and port number information embedded in the data stream. When a device behind the ZyWALL uses an application for which the ZyWALL has ALG service enabled, the ZyWALL translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and dynamically creates implicit NAT port forwarding and firewall rules for the application's traffic to come in from the WAN to the LAN.

21.1.1 ALG and NAT

The ZyWALL dynamically creates an implicit NAT session for the application's traffic from the WAN to the LAN.

The ALG on the ZyWALL supports all NAT mapping types, including **One to One**, **Many to One**, **Many to Many Overload** and **Many One to One**.

21.1.2 ALG and the Firewall

The ZyWALL uses the dynamic port that the session uses for data transfer in creating an implicit temporary firewall rule for the session's traffic. The firewall rule only allows the session's traffic to go through in the direction that the ZyWALL determines from its inspection of the data payload of the application's packets. The firewall rule is automatically deleted after the application's traffic has gone through.

21.2 FTP

File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. The FTP ALG allows TCP packets with a port 21 destination to pass through. If the FTP server is located on the LAN, you must also configure NAT port forwarding and firewall rules if you want to allow access to the server from the WAN.

21.3 H.323

H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. NetMeeting uses H.323.

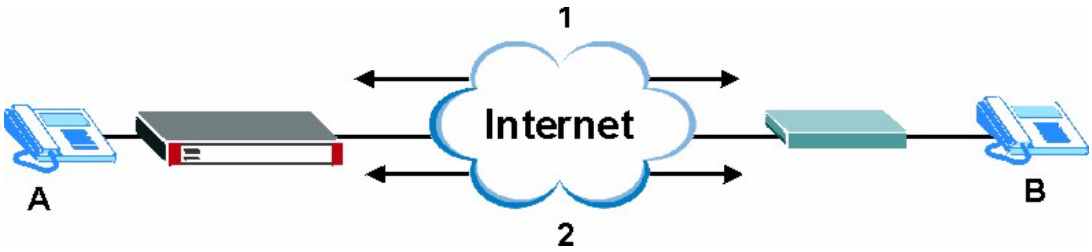
21.4 RTP

When you make a VoIP call using H.323 or SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

21.4.1 H.323 ALG Details

- The H.323 ALG supports peer-to-peer H.323 calls.
- The H.323 ALG handles H.323 calls that go through NAT or that the ZyWALL routes. You can also make other H.323 calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The H.323 ALG allows calls to go out through NAT. For example, you could make a call from a private IP address on the LAN to a peer device on the WAN.
- You must configure the firewall and port forwarding to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN. The following example shows H.323 signaling (1) and audio (2) sessions between H.323 devices A and B.

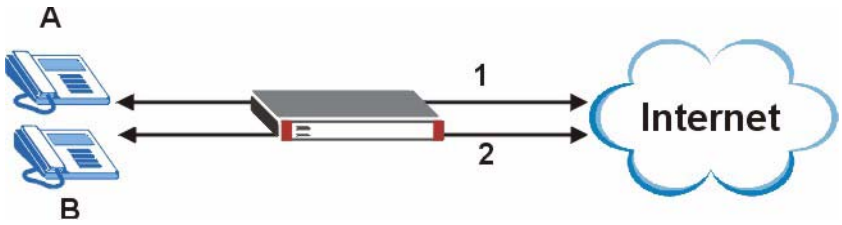
Figure 206 H.323 ALG Example



With multiple WAN IP addresses on the ZyWALL, you can configure different firewall and NAT **Many One to One** rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN. Use NAT **Many One to One** address mapping to have the H.323 calls from each of those LAN IP addresses go out through the same WAN IP address that calls come in on. The NAT **Many One to One** address mapping lets the ZyWALL correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure firewall and NAT **Many One to One** rules to allow LAN IP address **A** to receive calls through public WAN IP address **1**. You configure different firewall and NAT **Many One to One** rules to allow LAN IP address **B** to receive calls through public WAN IP address **2**. You configure corresponding NAT **Many One to One** address mapping to have calls from LAN IP address **A** go out through WAN IP address **1** and calls from LAN IP address **B** go out through WAN IP address **2**.

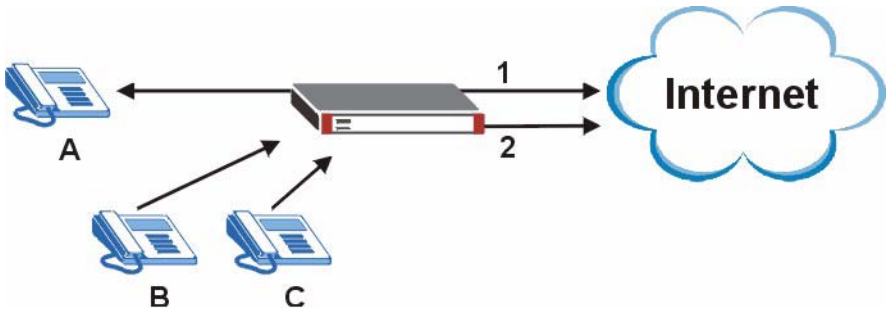
Figure 207 H.323 with Multiple WAN IP Addresses



- When you configure the firewall and NAT **Many One to One** address mapping to allow calls from the WAN to a specific IP address on the LAN, you can also use NAT **Many One to One** address mapping to have H.323 calls from other LAN IP addresses go out through a different WAN IP address. The NAT address mapping lets the ZyWALL correctly forward the return traffic for the calls initiated from the LAN IP addresses.

  For example, you configure the firewall and NAT **Many One to One** address mapping to allow LAN IP address **A** to receive calls from the Internet through WAN IP address **1**. You also use NAT **Many One to One** address mapping to have LAN IP address **A** make calls out through WAN IP address **1**. Configure another NAT **Many One to One** address mapping entry to have H.323 calls from LAN IP addresses **B** and **C** go out through WAN IP address **2**. Even though only LAN IP address **A** can receive incoming calls from the Internet, LAN IP addresses **B** and **C** can still make calls out to the Internet.

Figure 208 H.323 Calls from the WAN with Multiple Outgoing Calls



- The H.323 ALG operates on TCP packets with a port 1720 destination.
- The ZyWALL allows H.323 audio connections.

21.5 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

21.5.1 STUN

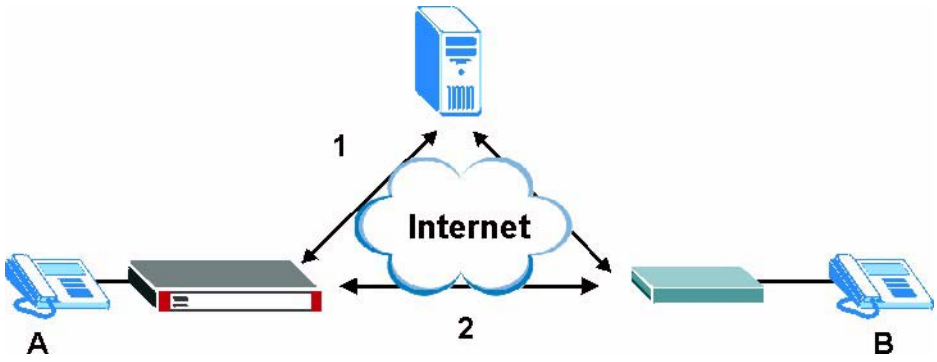
STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the VoIP device to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the VoIP device to find the public IP address that NAT assigned, so the VoIP device can embed it in the SIP data stream. See RFC 3489 for details on STUN. You do not need to use STUN for devices behind the ZyWALL if you enable the SIP ALG.

21.5.2 SIP ALG Details

- SIP clients can be connected to the LAN. A SIP server must be on the WAN.
- You can make and receive calls between the LAN and the WAN. You cannot make a call between the LAN and the LAN.
- The SIP ALG allows UDP packets with a port 5060 destination to pass through.
- The ZyWALL allows SIP audio connections.

The following example shows SIP signaling (**1**) and audio (**2**) sessions between SIP clients **A** and **B** and the SIP server.

Figure 209 SIP ALG Example



21.5.3 SIP Signaling Session Timeout

Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the ZyWALL.

If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout default (60 minutes), the ZyWALL SIP ALG drops any incoming calls after the timeout period.

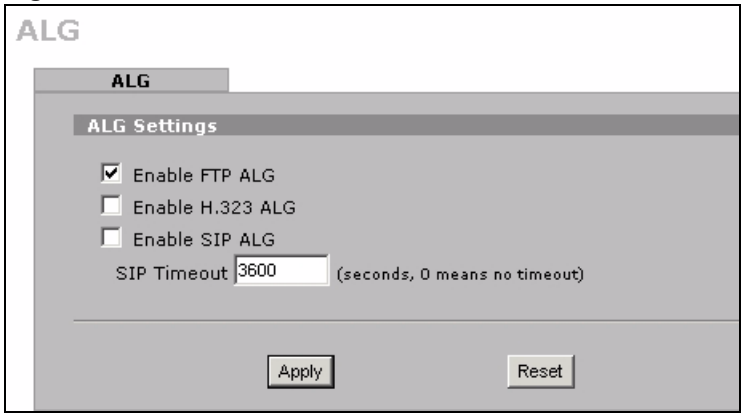
21.5.4 SIP Audio Session Timeout

If no voice packets go through the SIP ALG before the timeout period (default 5 minutes) expires, the SIP ALG does not drop the call but blocks all voice traffic and deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

21.6 ALG Screen

Click **ADVANCED > ALG** to open the **ALG** screen. Use the **ALG** screen to turn individual ALGs off or on and set the SIP timeout.

Figure 210 ADVANCED > ALG



The following table describes the labels in this screen.

Table 106 ADVANCED > ALG

LABEL	DESCRIPTION
Enable FTP ALG	Select this check box to allow FTP sessions to pass through the ZyWALL. FTP (File Transfer Program) is a program that enables fast transfer of files, including large files that may not be possible by e-mail.
Enable H.323 ALG	Select this check box to allow H.323 sessions to pass through the ZyWALL. H.323 is a protocol used for audio communications over networks.
Enable SIP ALG	Select this check box to allow SIP sessions to pass through the ZyWALL. SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol.
SIP Timeout	Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the ZyWALL. If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout (default 60 minutes), the ZyWALL SIP ALG drops any incoming calls after the timeout period. Enter the SIP signaling session timeout value.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

PART V
Reports, Logs and Maintenance

Reports (339)
Logs (351)
Maintenance (375)

22

Reports

This chapter contains information about the ZyWALL's system and reports.

22.1 Configuring Reports

The **Reports** screens display statistics about network usage, IDP and anti-virus statistics. You can also configure how reports are emailed in this section.

22.2 Traffic Statistics Screen

Click **REPORTS** to display the following screen.

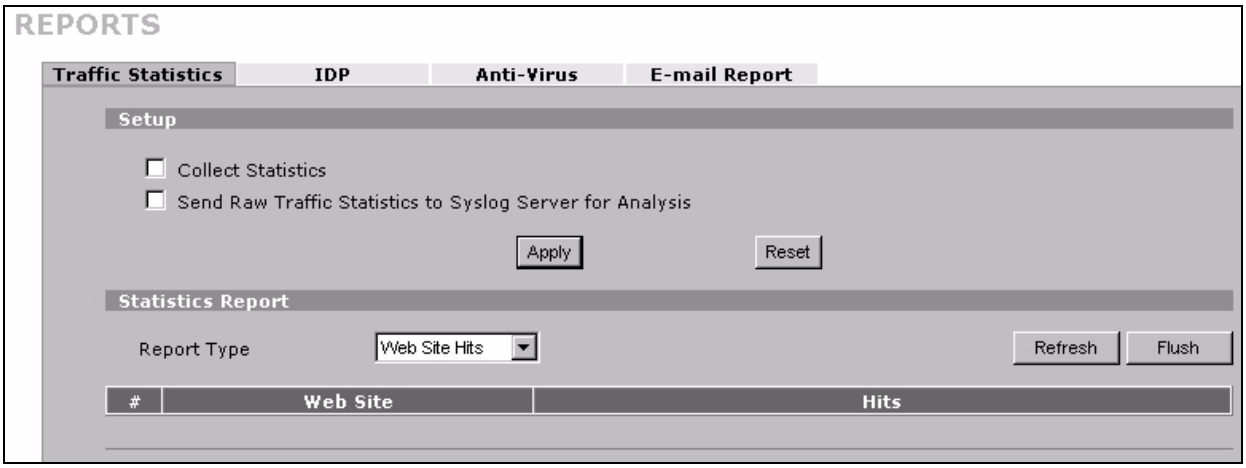
The **Traffic Statistics** screen displays which local computers send and receive the most traffic, what kinds of traffic are used the most and which web sites are visited the most often. The ZyWALL can record and display the following network usage details:

- Web sites visited the most often
- Number of times the most visited web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The IP addresses to and/or from which the most traffic has been sent
- How much traffic has been sent to and from the IP addresses to and/or from which the most traffic has been sent

The web site hit count may not be 100% accurate because sometimes when an individual web page loads, it may contain references to other web sites that also get counted as hits.

The ZyWALL records web site hits by counting the HTTP GET packets. Many web sites include HTTP GET references to other web sites and the ZyWALL may count these as hits, thus the web hit count is not (yet) 100% accurate.

Figure 211 REPORTS > Traffic Statistics



Enabling the ZyWALL's reporting function decreases the overall throughput by about 1 Mbps.

The following table describes the labels in this screen.

Table 107 REPORTS > Traffic Statistics

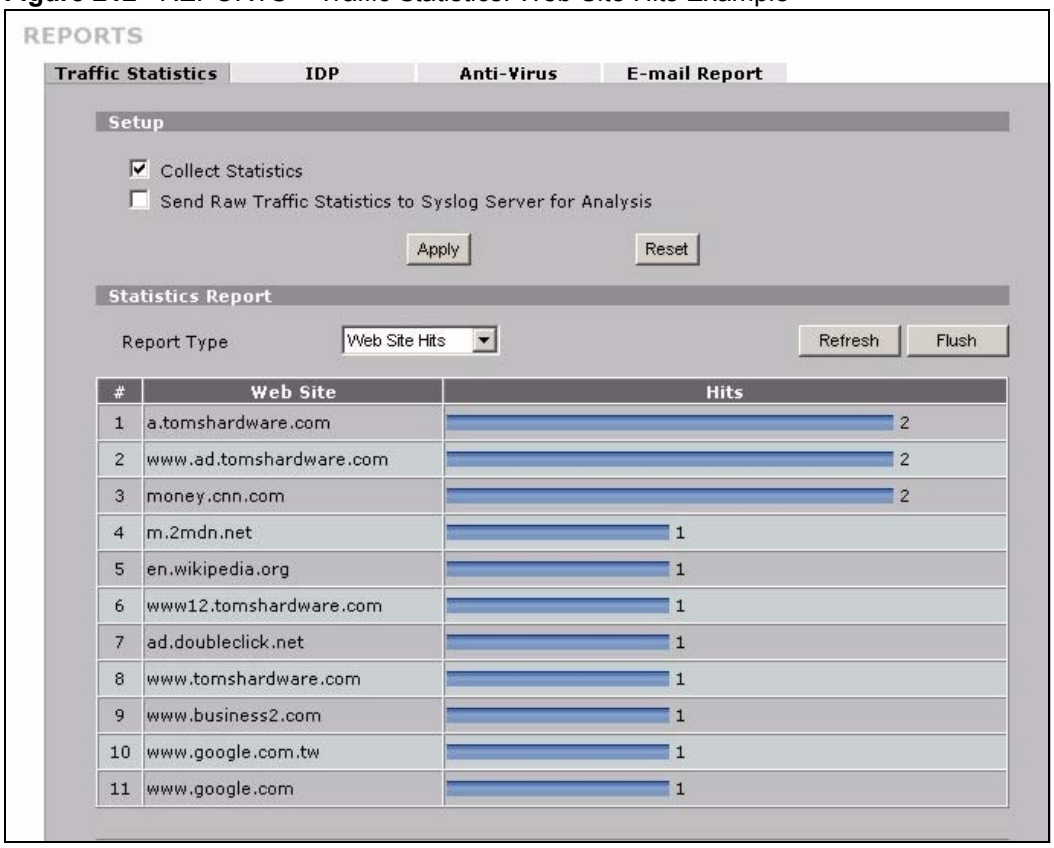
LABEL	DESCRIPTION
Collect Statistics	Select the check box and click **Apply** to have the ZyWALL record report data.
Send Raw Traffic Statistics to Syslog Server for Analysis	Select the check box and click **Apply** to have the ZyWALL send unprocessed traffic statistics to a syslog server for analysis. You must have the syslog server already configured in the **Log Settings** screen.
Apply	Click **Apply** to save your changes to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.
Report Type	Use the drop-down list box to select the type of reports to display. **Web Site Hits** displays the web sites that have been visited the most often from the LAN and how many times they have been visited. **Protocol/Port** displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports. **Host IP Address** displays the IP addresses to and /or from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses.
Refresh	Click **Refresh** to update the report display. The report also refreshes automatically when you close and reopen the screen.
Flush	Click **Flush** to discard the old report data and update the report display.

All of the recorded reports data is erased when you turn off the ZyWALL.

22.2.1 Viewing Web Site Hits

In the **Traffic Statistics** screen, select **Web Site Hits** from the **Report Type** drop-down list box to have the ZyWALL record and display which web sites have been visited the most often and how many times they have been visited.

Figure 212 REPORTS > Traffic Statistics: Web Site Hits Example



The following table describes the label in this screen.

Table 108 REPORTS > Traffic Statistics: Web Site Hits Report

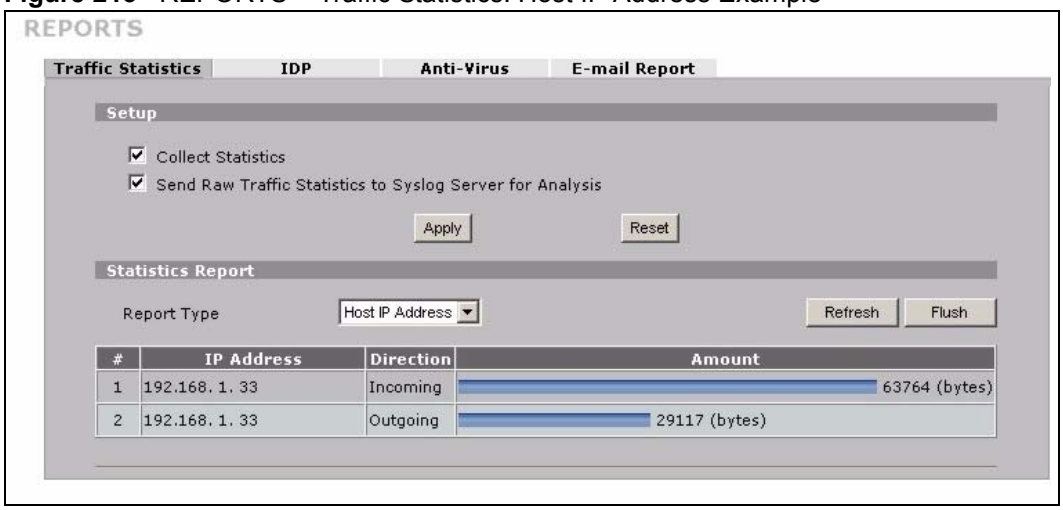
LABEL	DESCRIPTION
Web Site	This column lists the domain names of the web sites visited most often from computers on the LAN. The names are ranked by the number of visits to each web site and listed in descending order with the most visited web site listed first. The ZyWALL counts each page viewed in a web site as another hit on the web site.
Hits	This column lists how many times each web site has been visited. The count starts over at 0 if a web site passes the hit count limit (see Table 111 on page 343).

22.2.2 Viewing Host IP Address

In the **Traffic Statistics** screen, select **Host IP Address** from the **Report Type** drop-down list box to have the ZyWALL record and display the IP addresses that the most traffic has been sent to and/or from and how much traffic has been sent to and/or from those IP addresses.

Computers take turns using dynamically assigned IP addresses. The ZyWALL continues recording the bytes sent to or from a IP address when it is assigned to a different computer.

Figure 213 REPORTS > Traffic Statistics: Host IP Address Example



The following table describes the labels in this screen.

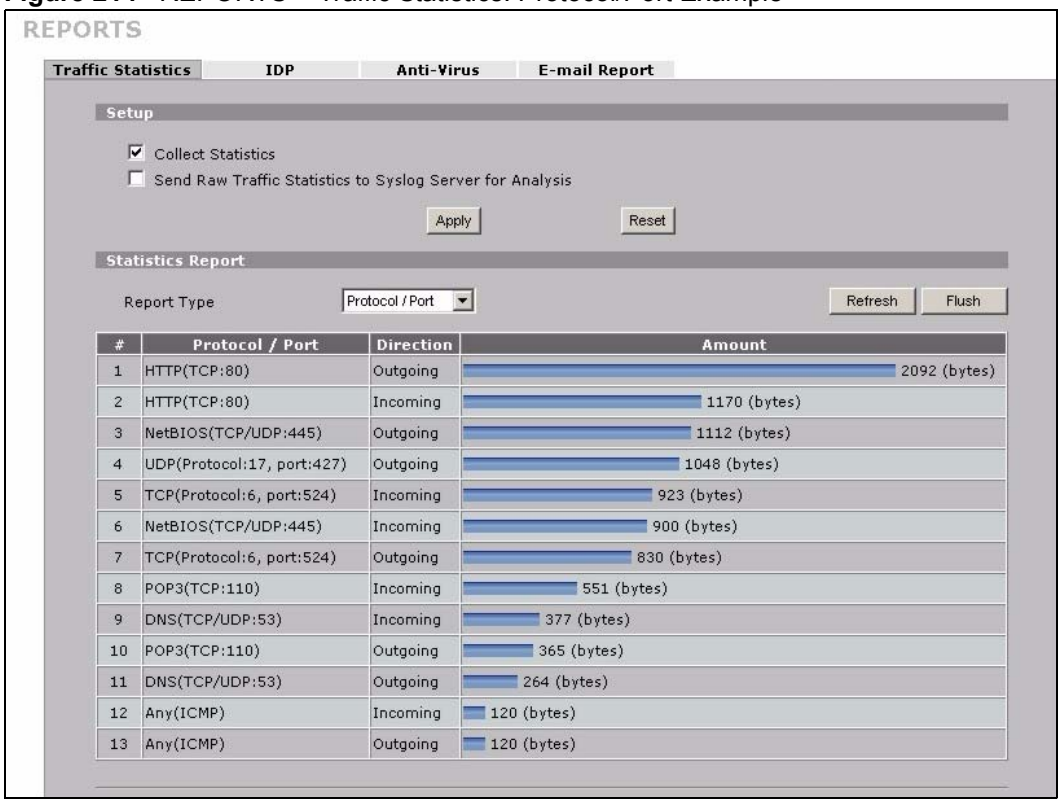
Table 109 REPORTS > Traffic Statistics: Host IP Address

LABEL	DESCRIPTION
IP Address	This column lists the IP addresses to and/or from which the most traffic has been sent. The addresses are listed in descending order with the IP address to and/or from which the most traffic was sent listed first.
Direction	This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN. This field displays **Outgoing** to denote traffic that is going out from the LAN to the WAN.
Amount	This column displays how much traffic has gone to and from the listed IP addresses. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic sent to and from the IP address. The count starts over at 0 if the total traffic sent to and from a IP passes the bytes count limit (see Table 111 on page 343).

22.2.3 Viewing Protocol/Port

In the **Traffic Statistics** screen, select **Protocol/Port** from the **Report Type** drop-down list box to have the ZyWALL record and display which protocols or service ports have been used the most and the amount of traffic for the most used protocols or service ports.

Figure 214 REPORTS > Traffic Statistics: Protocol/Port Example



The following table describes the labels in this screen.

Table 110 REPORTS > Traffic Statistics: Protocol/ Port

LABEL	DESCRIPTION
Protocol/Port	This column lists the protocols or service ports for which the most traffic has gone through the ZyWALL. The protocols or service ports are listed in descending order with the most used protocol or service port listed first.
Direction	This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN. This field displays **Outgoing** to denote traffic that is going out from the LAN to the WAN.
Amount	This column lists how much traffic has been sent and/or received for each protocol or service port. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit (see Table 111 on page 343).

22.2.4 System Reports Specifications

The following table lists detailed specifications on the reports feature.

Table 111 Report Specifications

LABEL	DESCRIPTION
Number of web sites/protocols or ports/IP addresses listed:	20

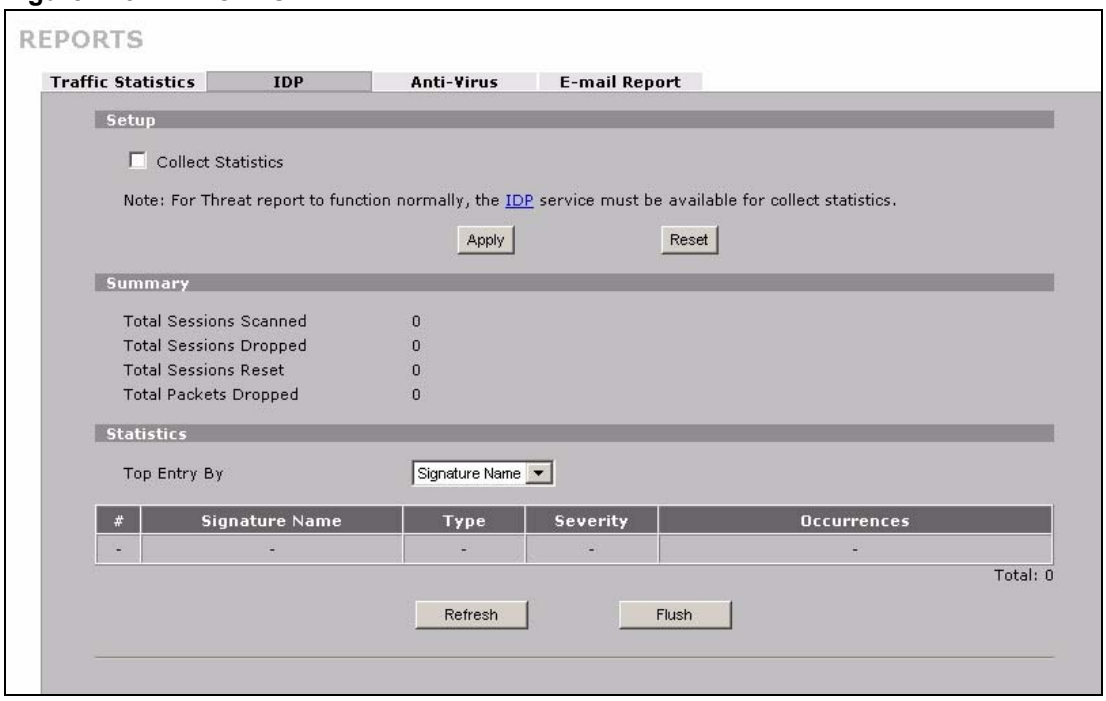
Table 111 Report Specifications

LABEL	DESCRIPTION
Hit count limit:	Up to 2^{32} hits can be counted per web site. The count starts over at 0 if it passes four billion.
Bytes count limit:	Up to 2^{64} bytes can be counted per protocol/port or LAN IP address. The count starts over at 0 if it passes 2^{64} bytes.

22.3 IDP Screen

Click **REPORTS > IDP** to display the **IDP** screen. This screen displays IDP (Intrusion Detection and Prevention) statistics.

Figure 215 REPORTS > IDP



The following table describes the labels in this screen.

Table 112 REPORTS > IDP

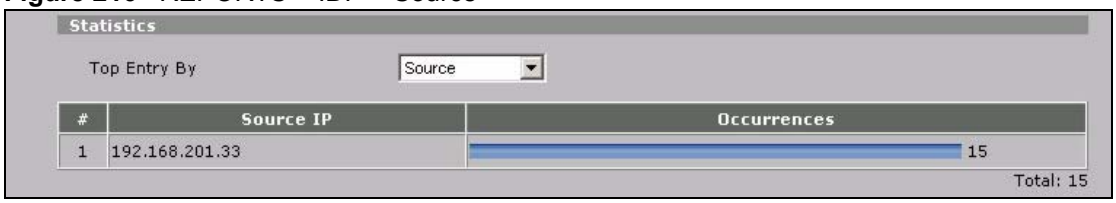
LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the ZyWALL collect IDP statistics. The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the ZyWALL or click the **Flush** button. Collecting starts over and a new collection start time displays.
Total Sessions Scanned	This field displays the number of sessions that the ZyWALL has checked for intrusion characteristics.
Total Sessions Dropped	The ZyWALL can detect and drop malicious sessions from network traffic. This field displays the number of sessions that the ZyWALL has dropped.
Total Sessions Reset	The ZyWALL can detect and reset suspicious network traffic sessions. This field displays the number of sessions that the ZyWALL has reset.

Table 112 REPORTS > IDP (continued)

LABEL	DESCRIPTION
Total Packets Dropped	The ZyWALL can detect and drop malicious packets from network traffic. This field displays the number of packets that the ZyWALL has dropped.
Top Entry By	Use this field to have the following (read-only) table display the top IDP entries by **Signature Name**, **Source** or **Destination**. Select **Signature Name** to list the most common signatures that the ZyWALL has detected. Select **Source** to list the source IP addresses from which the ZyWALL has detected the most intrusion attempts. Select **Destination** to list the most common destination IP addresses for intrusion attempts that the ZyWALL has detected.
#	This field displays the entry's rank in the list of the top entries.
Signature Name	This column displays when you display the entries by **Signature Name**. The signature name identifies a specific intrusion pattern. Click the hyperlink for more detailed information on the intrusion.
Type	This column displays when you display the entries by **Signature Name**. It shows the categories of intrusions. See Table 78 on page 282 for more information.
Severity	This column displays when you display the entries by **Signature Name**. It shows the level of threat that the intrusions may pose. See Table 79 on page 283 for more information.
Source IP	This column displays when you display the entries by **Source.** It shows the source IP address of the intrusion attempts.
Destination IP	This column displays when you display the entries by **Destination.** It shows the destination IP address at which intrusion attempts were targeted.
Occurrences	This field displays how many times the ZyWALL has detected the event described in the entry.
Total	This field displays the sum of the occurrences of the events in the entries.
Refresh	Click **Refresh** to update the report display with additional information that the ZyWALL may have collected while you had the screen open. The report also refreshes automatically when you close and reopen the screen.
Flush	Click **Flush** to discard the report data and restart collecting statistics.

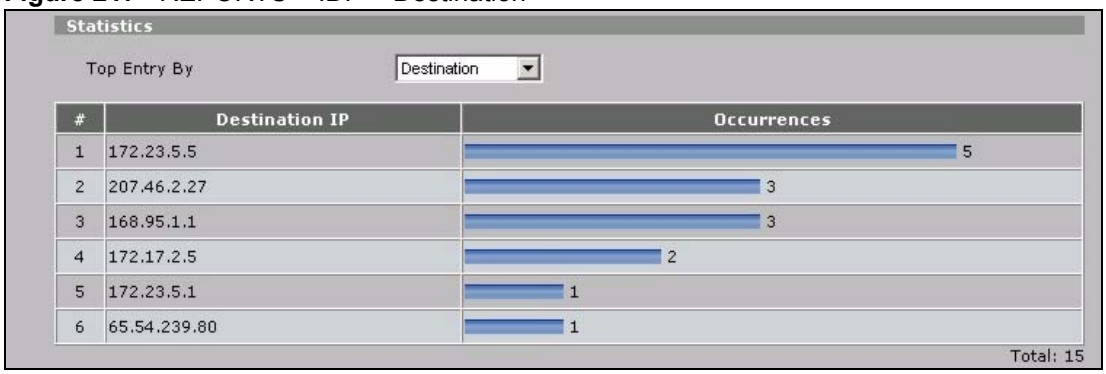
The statistics display as follows when you display the top entries by source.

Figure 216 REPORTS > IDP > Source



The statistics display as follows when you display the top entries by destination.

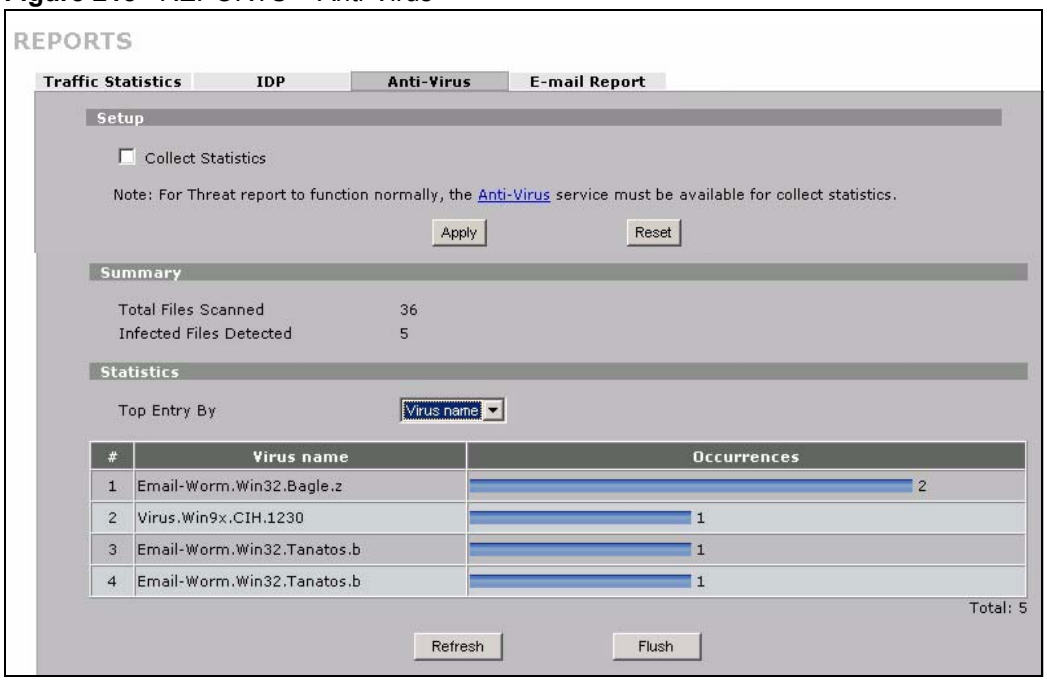
Figure 217 REPORTS > IDP > Destination



22.4 Anti-Virus Screen

Click **REPORTS > Anti-Virus** to display the **Anti-Virus** screen. This screen displays anti-virus statistics.

Figure 218 REPORTS > Anti-Virus



The following table describes the labels in this screen.

Table 113 REPORTS > Anti-Virus

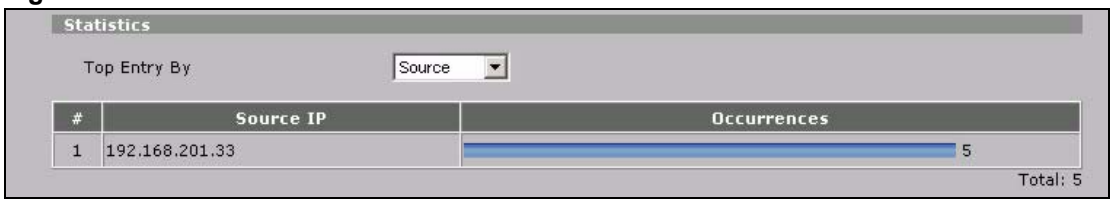
LABEL	DESCRIPTION
Collect Statistics	Select this check box to have the ZyWALL collect anti-virus statistics. The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the ZyWALL or click the **Flush** button. Collecting starts over and a new collection start time displays.
Total Files Scanned	This field displays the number of files that the ZyWALL has scanned for viruses.

Table 113 REPORTS > Anti-Virus (continued)

LABEL	DESCRIPTION
Infected Files Detected	This field displays the number of files in which the ZyWALL has detected a virus.
Top Entry By	Use this field to have the following (read-only) table display the top anti-virus entries by **Virus Name**, **Source** or **Destination**. Select **Virus Name** to list the most common viruses that the ZyWALL has detected. Select **Source** to list the source IP addresses from which the ZyWALL has detected the most virus-infected files. Select **Destination** to list the most common destination IP addresses for virus-infected files that ZyWALL has detected.
#	This field displays the entry's rank in the list of the top entries.
Virus name	This column displays when you display the entries by **Virus Name**. This displays the name of a detected virus.
Source IP	This column displays when you display the entries by **Source.** It shows the source IP address of virus-infected files that the ZyWALL has detected.
Destination IP	This column displays when you display the entries by **Destination.** It shows the destination IP address of virus-infected files that the ZyWALL has detected.
Occurrences	This field displays how many times the ZyWALL has detected the event described in the entry.
Total	This field displays the sum of the occurrences of the events in the entries.
Refresh	Click **Refresh** to update the report display with additional information that the ZyWALL may have collected while you had the screen open. The report also refreshes automatically when you close and reopen the screen.
Flush	Click **Flush** to discard the report data and restart collecting statistics.

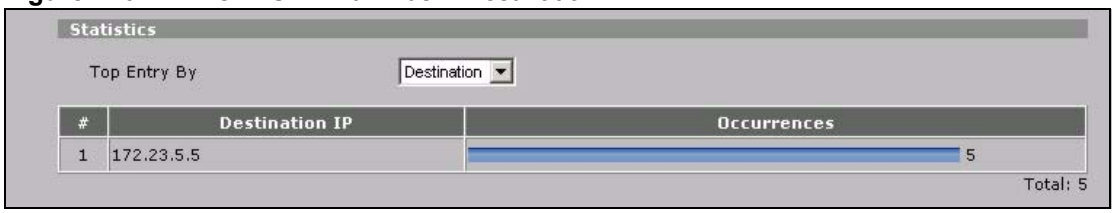
The statistics display as follows when you display the top entries by source.

Figure 219 REPORTS > Anti-Virus > Source



The statistics display as follows when you display the top entries by destination.

Figure 220 REPORTS > Anti-Virus > Destination

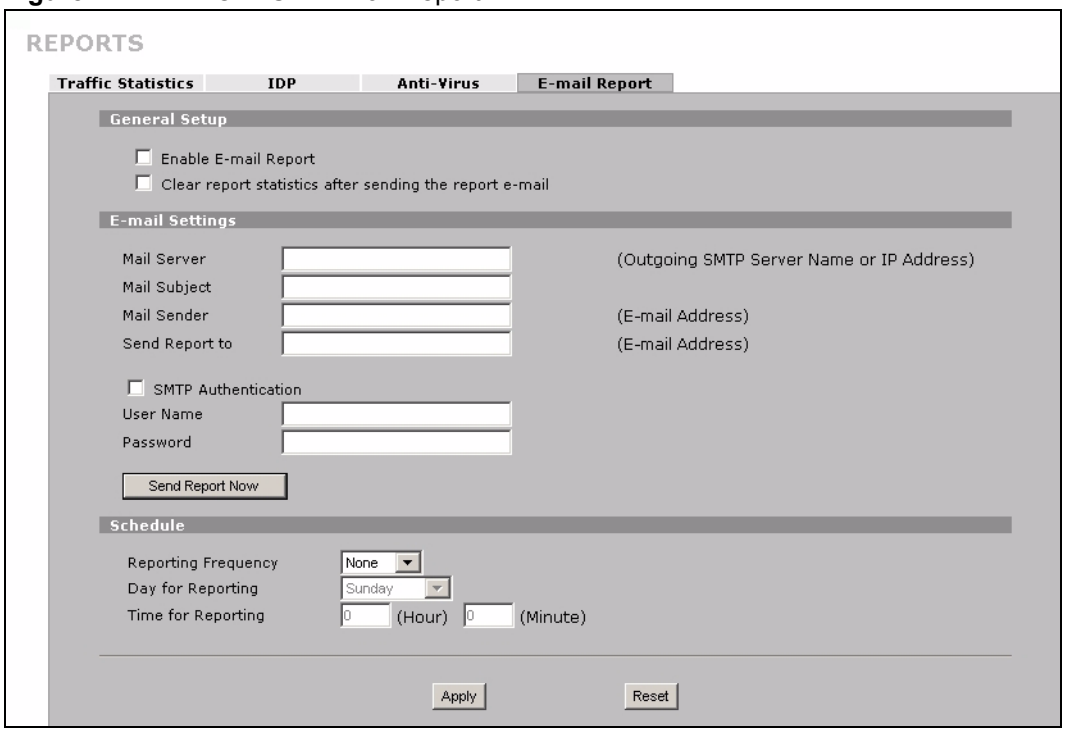


22.5 E-mail Report Screen

You can configure the ZyWALL to email a report including the information on network traffic, IDP, and anti-virus statistics provided in the report screens.

Click **REPORTS > E-mail Report** to display the following screen.

Figure 221 REPORTS > E-mail Report



The following table describes the labels in this screen.

Table 114 REPORTS > E-mail Report

LABEL	DESCRIPTION
General Setup	
Enable E-mail Report	Select this to turn on the e-mail report feature. You must then specify a valid e-mail server in order to send reports.
Clear report statistics after sending the report e-mail	Select this to clear current records of IDP and anti-virus statistics (available in the **Reports** screens) once the report has been sent.
E-mail Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail address specified in the **Mail Sender** field. If this field is left blank, report files will not be sent via e-mail.
Mail Subject	Type a descriptive subject here to be included in the report e-mail subject header.
Mail Sender	Enter the e-mail address that you want to be in the from/sender line of the diagnostic e-mail message that the ZyWALL sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well.
Send Report to	Report files are sent to the e-mail address specified in this field. If this field is left blank, report files will not be sent via e-mail.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the report files.
User Name	Enter the user name (up to 63 characters) (usually the user name of a mail account you specified in the **Mail Sender** field).

Table 114 REPORTS > E-mail Report (continued)

LABEL	DESCRIPTION
Password	Enter the password associated with the user name above.
Send Report Now	Click this to send the report e-mail immediately.
Schedule	
Reporting Frequency	Select the frequency of the report e-mail from the drop-down box. Options are **None**, **Hourly**, **Daily** and **Weekly**. If you select **Daily** or **Weekly**, specify a time of day for the ZyWALL to generate and send diagnostic e-mails. If you select **Weekly**, then also specify which day of the week. Select **None** to have the ZyWALL not generate and send diagnostic e-mails based on a time period.
Day for Reporting	If **Weekly** is selected in the **Schedule** field, select the day for reporting from the drop-down box.
Time for Reporting	If **Daily** or **Weekly** is selected in the **Schedule** field, type the hour and minute in 24-hour format (for example, 23:00 equals 11:00 pm) to send the report email in these two boxes.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

23

Logs

This chapter contains information about configuring general log settings and viewing the ZyWALL's logs. Refer to Section 23.3.1 on page 357 for example log message explanations.

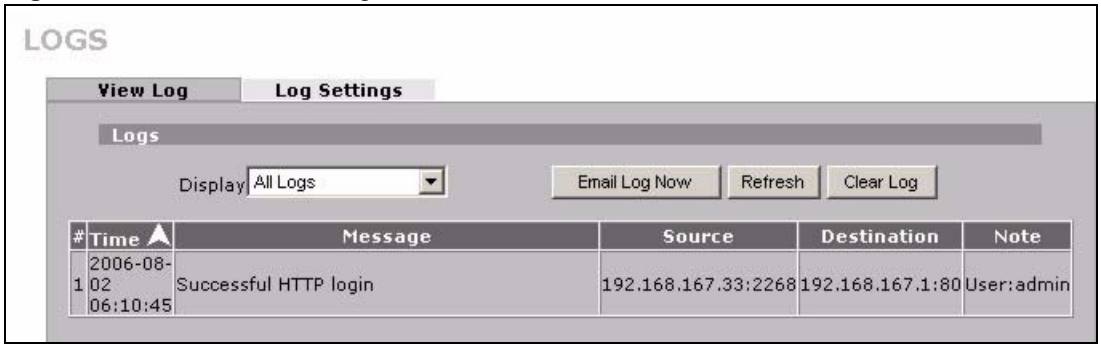
23.1 View Log

The web configurator allows you to look at all of the ZyWALL's logs in one location.

Click **LOGS** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 23.3 on page 353). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 222 LOGS > View Log



The following table describes the labels in this screen.

Table 115 LOGS > View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** page (see Section 23.3 on page 353) display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Log Settings**, see Section 23.3 on page 353).
Refresh	Click **Refresh** to renew the log screen.

Table 115 LOGS > View Log (continued)

LABEL	DESCRIPTION
Clear Log	Click **Clear Log** to delete all the logs.
#	This field displays the log number.
Time	This field displays the time the log was recorded. See Section 24.6 on page 378 to configure the ZyWALL's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.

23.2 Log Description Example

The following is an example of how a log displays in the command line interpreter and a description of the sample log. Refer to the appendices for more log message descriptions and details on using the command line interpreter to display logs.

```
#  .time                source                destination
notes
    message
  5|06/08/2004 05:58:20 |172.21.4.187:137      |172.21.255.255:137
|ACCESS BLOCK
    Firewall default policy: UDP (W to W/ZW)
```

Table 116 Log Description Example

LABEL	DESCRIPTION
#	This is log number five.
time	The log was generated on June 8, 2004 at 5:58 and 20 seconds AM.
source	The log was generated due to a NetBIOS packet sent from IP address 172.21.4.187 port 137.
destination	The NetBIOS packet was sent to the 172.21.255.255 subnet port 137. This was a NetBIOS UDP broadcast packet meant to discover devices on the network.
notes	The ZyWALL blocked the packet.
message	The ZyWALL blocked the packet in accordance with the firewall's default policy of blocking sessions that are initiated from the WAN. "UDP" means that this was a User Datagram Protocol packet. "W to W/ZW" indicates that the packet was traveling from the WAN to the WAN or the ZyWALL.

23.2.1 About the Certificate Not Trusted Log

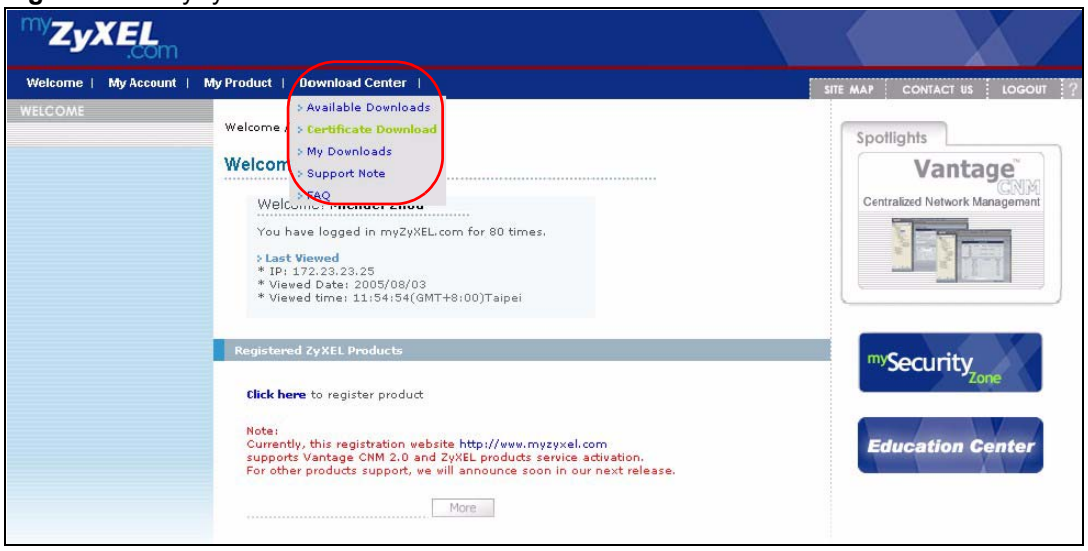
myZyXEL.com and the update server use certificates signed by VeriSign to identify themselves. If the ZyWALL does not have a CA certificate signed by VeriSign as a trusted CA, the ZyWALL will not trust the certificate from myZyXEL.com and the update server. The ZyWALL will generate a log like "Due to error code(11), cert not trusted: SSL/TLS peer certif..." for every time it attempt to establish a (HTTPS) connection with myZyXEL.com and

the update server. The V4.00 default configuration file includes a trusted CA certificate signed by VeriSign. If you upgraded to ZyNOS V4.00 firmware without uploading the V4.00 default configuration file, you can download a CA certificate signed by VeriSign from myZyXEL.com and import it into the ZyWALL as a trusted CA. This will stop the ZyWALL from generating this log every time it attempts to connect with myzyxel.com and the update server.

Follow the steps below to download the certificate from myZyXEL.com.

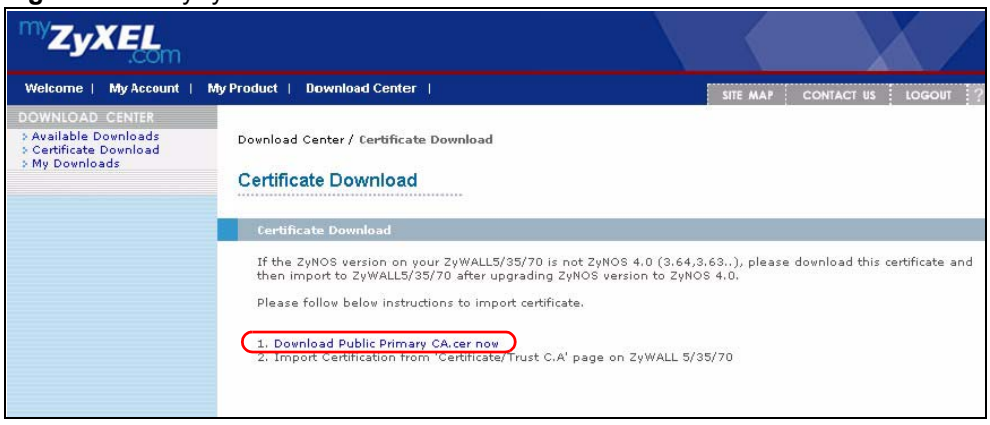
1. Go to http://www.myZyXEL.com and log in with your account.
2. Click **Download Center** and then **Certificate Download**.

Figure 223 myZyXEL.com: Download Center



3. Click the link in the **Certificate Download** screen.

Figure 224 myZyXEL.com: Certificate Download


Welcome | My Account | My Product | Download Center |
SITE MAP | CONTACT US | LOGOUT
DOWNLOAD CENTER
Available Downloads
Certificate Download
My Downloads
Download Center / Certificate Download
Certificate Download
Certificate Download
If the ZyNOS version on your ZyWALL5/35/70 is not ZyNOS 4.0 (3.64,3.63..), please download this certificate and then import to ZyWALL5/35/70 after upgrading ZyNOS version to ZyNOS 4.0.
Please follow below instructions to import certificate.
1. Download Public Primary CA.cer now
2. Import Certification from 'Certificate/Trust C.A' page on ZyWALL 5/35/70

23.3 Configuring Log Settings

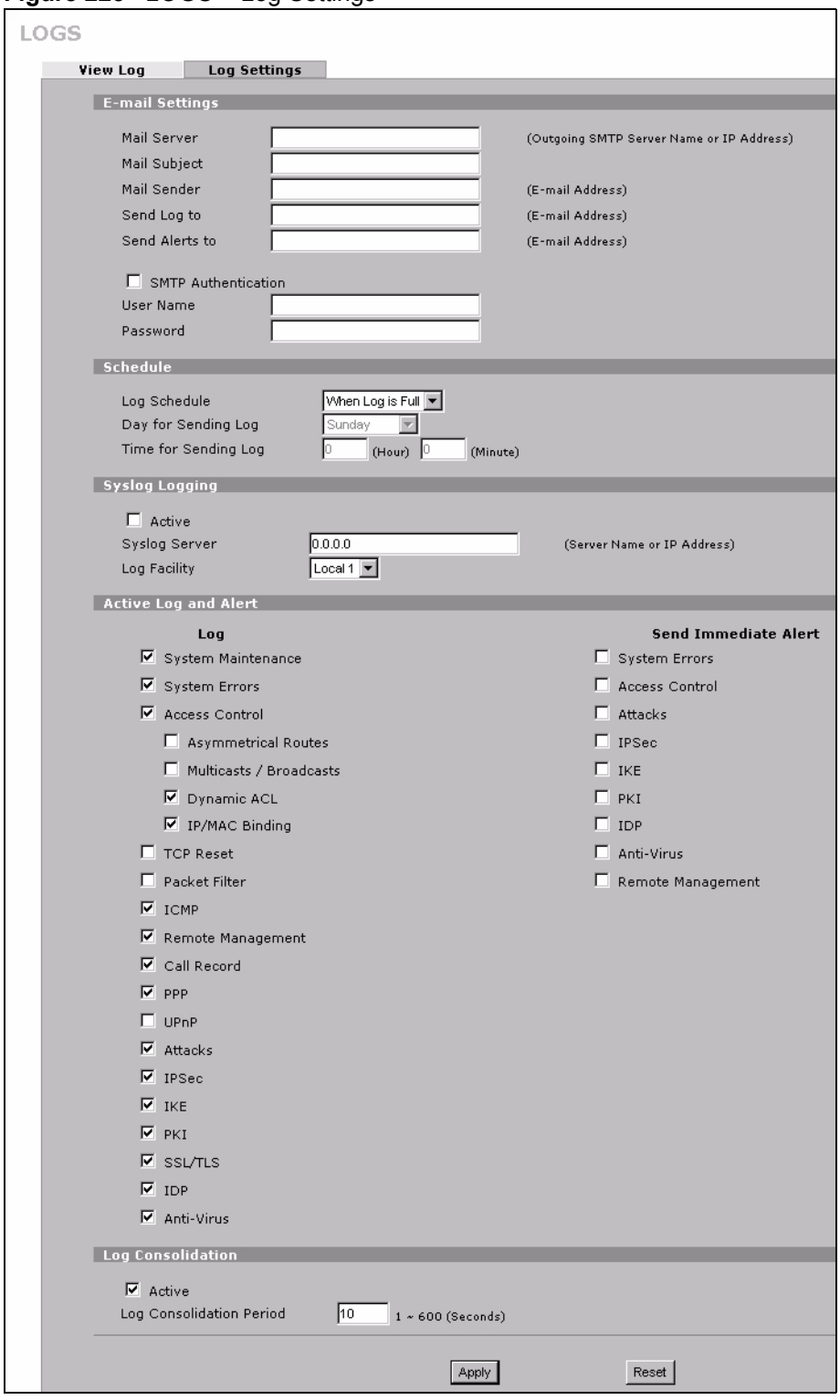
To change your ZyWALL's log settings, click **LOGS** > **Log Settings**. The screen appears as shown.

Use the **Log Settings** screen to configure to where the ZyWALL is to send logs; the schedule for when the ZyWALL is to send the logs and which logs and/or immediate alerts the ZyWALL is to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 225 LOGS > Log Settings



The following table describes the labels in this screen.

Table 117 LOGS > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyWALL sends.
Mail Sender	Enter the e-mail address that you want to be in the from/sender line of the log e-mail message that the ZyWALL sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well.
Send Log To	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.
User Name	Enter the user name (up to 63 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Schedule	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: **Daily** **Weekly** **Hourly** **When Log is Full** **None**. If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Syslog Logging	Syslog allows you to send system logs to a server. Syslog logging sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Active Log and Alert	
Log	Select the categories of logs that you want to record. Logs include alerts.

Table 117 LOGS > Log Settings (continued)

LABEL	DESCRIPTION
Send Immediate Alert	Select the categories of alerts for which you want the ZyWALL to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field.
Log Consolidation	
Active	Some logs (such as the Attacks logs) may be so numerous that it becomes easy to ignore other important log messages. Select this check box to merge logs with identical messages into one log. You can use the `sys log consolidate msglist` command to see what log messages will be consolidated.
Log Consolidation Period	Specify the time interval during which the ZyWALL merges logs with identical messages into one log.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

23.3.1 Log Descriptions

This section provides descriptions of example log messages.

Table 118 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`WAN interface gets IP: %s`	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns %s`	The DHCP server assigned an IP address to a client.
`Successful WEB login`	Someone has logged on to the router's web configurator interface.
`WEB login failed`	Someone has failed to log on to the router's web configurator interface.
`Successful TELNET login`	Someone has logged on to the router via telnet.
`TELNET login failed`	Someone has failed to log on to the router via telnet.
`Successful FTP login`	Someone has logged on to the router via FTP.
`FTP login failed`	Someone has failed to log on to the router via FTP.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.
`Starting Connectivity Monitor`	Starting Connectivity Monitor.
`Time initialized by Daytime Server`	The router got the time and date from the Daytime server.
`Time initialized by Time server`	The router got the time and date from the time server.
`Time initialized by NTP server`	The router got the time and date from the NTP server.

Table 118 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
Connect to Daytime server fail	The router was not able to connect to the Daytime server.
Connect to Time server fail	The router was not able to connect to the Time server.
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
Configuration Change: PC = 0x%x, Task ID = 0x%x	The router is saving configuration changes.
Successful SSH login	Someone has logged on to the router's SSH server.
SSH login failed	Someone has failed to log on to the router's SSH server.
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.
DNS server %s was not responding to last 32 consecutive queries…	The specified DNS server did not respond to the last 32 consecutive queries.
DDNS update IP:%s (host %d) successfully	The device updated the IP address of the specified DDNS host name.
SMTP successfully	The device sent an e-mail.
myZyXEL.com registration successful	Registration of the device with myZyXEL.com was successful.
Trial service registration successful	Registration for a trial service was successful.
Service upgrade successful	Registration for a service upgrade was successful.
Service refresh successful.	The device successfully refreshed service information from myZyXEL.com.
IDP/Anti-Virus trial service activation successfully	The IDP and anti-virus trial service was successfully activated for this device.
%s	The myZyXEL.com service registration failed due to the error listed. If you are unable to register for services at myZYXEL.com, the error message displayed in this log may be useful when contacting customer support.

Table 119 System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.

Table 119 System Error Logs (continued)

LOG MESSAGE	DESCRIPTION
DHCP Server cannot assign the static IP %S (out of range).	The LAN subnet, LAN alias 1, or LAN alias 2 was changed and the specified static DHCP IP addresses are no longer valid.
The DHCP static IP %s is conflict.	The static DHCP IP address conflicts with another host.
SMTP fail (%s)	The device failed to send an e-mail (error message included).
SMTP authentication fail (%s)	The device failed to authenticate with the SMTP server (error message included).

Table 120 Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.
Exceed maximum sessions per host (%d).	The device blocked a session because the host's connections exceeded the maximum sessions per host.
Firewall allowed a packet that matched a NAT session: [TCP | UDP]	A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN.

Table 121 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.

Table 121 TCP Reset Logs (continued)

LOG MESSAGE	DESCRIPTION
`Firewall session time out, sent TCP RST`	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
`Exceed MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > “Maximum Incomplete High”, the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < “Maximum Incomplete Low”.
`Access block, sent TCP RST`	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "sys firewall tcprst").

Table 122 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
`[ TCP | UDP | ICMP | IGMP | Generic ] packet filter matched (set: %d, rule: %d)`	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

For type and code details, see Table 136 on page 370.

Table 123 ICMP Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	ICMP access matched (or didn’t match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
`Triangle route packet forwarded: ICMP`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn’t have a corresponding NAT table entry.
`Unsupported/out-of-order ICMP: ICMP`	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 124 CDR Logs

LOG MESSAGE	DESCRIPTION
board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s	The router received the setup requirements for a call. “call” is the reference (count) number of the call. “dev” is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or “ch” is the call channel ID. For example,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.
board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s	The PPPoE, PPTP or dial-up call is connected.
board %d line %d channel %d, call %d, %s C02 Call Terminated	The PPPoE, PPTP or dial-up call was disconnected.

Table 125 PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection’s Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection’s Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection’s Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection’s Internet Protocol Control Protocol stage is starting.
ppp:IPCP Opening	The PPP connection’s Internet Protocol Control Protocol stage is opening.
ppp:LCP Closing	The PPP connection’s Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection’s Internet Protocol Control Protocol stage is closing.

Table 126 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

For type and code details, see Table 136 on page 370.

Table 127 Attack Logs

LOG MESSAGE	DESCRIPTION
attack [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack.
land [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack.

Table 127 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.
ports scan UDP	The firewall detected a UDP port scan attack.
Firewall sent TCP packet in response to DoS attack TCP	The firewall sent TCP packet in response to a DoS attack
ICMP Source Quench ICMP	The firewall detected an ICMP Source Quench attack.
ICMP Time Exceed ICMP	The firewall detected an ICMP Time Exceed attack.
ICMP Destination Unreachable ICMP	The firewall detected an ICMP Destination Unreachable attack.
ping of death. ICMP	The firewall detected an ICMP ping of death attack.
smurf ICMP	The firewall detected an ICMP smurf attack.
IP address in FTP port command is different from the client IP address. It maybe a bounce attack.	The IP address in an FTP port command is different from the client IP address. It may be a bounce attack.
Fragment packet size is smaller than the MTU size of output interface.	The fragment packet size is smaller than the MTU size of output interface.

Table 128 Remote Management Logs

LOG MESSAGE	DESCRIPTION
Remote Management: FTP denied	Attempted use of FTP service was blocked according to remote management settings.
Remote Management: TELNET denied	Attempted use of TELNET service was blocked according to remote management settings.
Remote Management: HTTP or UPnP denied	Attempted use of HTTP or UPnP service was blocked according to remote management settings.
Remote Management: WWW denied	Attempted use of WWW service was blocked according to remote management settings.
Remote Management: HTTPS denied	Attempted use of HTTPS service was blocked according to remote management settings.
Remote Management: SSH denied	Attempted use of SSH service was blocked according to remote management settings.
Remote Management: ICMP Ping response denied	Attempted use of ICMP service was blocked according to remote management settings.
Remote Management: SNMP denied	Attempted use of SNMP service was blocked according to remote management settings.
Remote Management: DNS denied	Attempted use of DNS service was blocked according to remote management settings.

Table 129 MAC Filter Logs

LOG MESSAGE	DESCRIPTION
MAC Filter Fail	The MAC filter blocked a device from connecting to the ZyWALL.
MAC Filter Success	The MAC filter allowed a device to connect to the ZyWALL.

Table 130 IPSec Logs

LOG MESSAGE	DESCRIPTION
Discard REPLAY packet	The router received and discarded a packet with an incorrect sequence number.
Inbound packet authentication failed	The router received a packet that has been altered. A third party may have altered or tampered with the packet.
Receive IPSec packet, but no corresponding tunnel exists	The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA.
Rule <%d> idle time out, disconnect	The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CI command to set the time period. The default value is 2 minutes.
WAN IP changed to <IP>	The router dropped all connections with the “MyIP” configured as “0.0.0.0” when the WAN IP address changed.
Inbound packet decryption failed	Please check the algorithm configuration.
Cannot find outbound SA for rule <%d>	A packet matches a rule, but there is no phase 2 SA for outbound traffic.

Table 130 IPSec Logs (continued)

LOG MESSAGE	DESCRIPTION
Rule [%s] sends an echo request to peer	The device sent a ping packet to check the specified VPN tunnel's connectivity.
Rule [%s] receives an echo reply from peer	The device received a ping response when checking the specified VPN tunnel's connectivity.

Table 131 IKE Logs

LOG MESSAGE	DESCRIPTION
Active connection allowed exceeded	The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached.
Start Phase 2: Quick Mode	Phase 2 Quick Mode has started.
Verifying Remote ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
Verifying Local ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
IKE Packet Retransmit	The router retransmitted the last packet sent because there was no response from the peer.
Failed to send IKE Packet	An Ethernet error stopped the router from sending IKE packets.
Too many errors! Deleting SA	An SA was deleted because there were too many errors.
Phase 1 IKE SA process done	The phase 1 IKE SA process has been completed.
Duplicate requests with the same cookie	The router received multiple requests from the same peer while still processing the first IKE packet from the peer.
IKE Negotiation is in process	The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet.
No proposal chosen	Phase 1 or phase 2 parameters don't match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail.
Local / remote IPs of incoming request conflict with rule <%d>	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
Cannot resolve Secure Gateway Addr for rule <%d>	The router couldn't resolve the IP address from the domain name that was used for the secure gateway address.
Peer ID: <peer id> <My remote type> -<My local type>	The displayed ID information did not match between the two ends of the connection.
vs. My Remote <My remote> -<My remote>	The displayed ID information did not match between the two ends of the connection.
vs. My Local <My local>-<My local>	The displayed ID information did not match between the two ends of the connection.
Send <packet>	A packet was sent. IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the log. Refer to Table 140 on page 374 for a list of ISAKMP payload types.

Table 131 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Recv <packet>	A packet was received. IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the log. Refer to Table 140 on page 374 for a list of ISAKMP payload types.
Recv <Main or Aggressive> Mode request from <IP>	The router received an IKE negotiation request from the peer address specified.
Send <Main or Aggressive> Mode request to <IP>	The router started negotiation with the peer.
Invalid IP <Peer local> / <Peer local>	The peer's "Local IP Address" is invalid.
Remote IP <Remote IP> / <Remote IP> conflicts	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
Phase 1 ID type mismatch	This router's "Peer ID Type" is different from the peer IPSec router's "Local ID Type".
Phase 1 ID content mismatch	This router's "Peer ID Content" is different from the peer IPSec router's "Local ID Content".
No known phase 1 ID type found	The router could not find a known phase 1 ID in the connection attempt.
ID type mismatch. Local / Peer: <Local ID type/Peer ID type>	The phase 1 ID types do not match.
ID content mismatch	The phase 1 ID contents do not match.
Configured Peer ID Content: <Configured Peer ID Content>	The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed.
Incoming ID Content: <Incoming Peer ID Content>	The phase 1 ID contents do not match and the incoming packet's ID content is displayed.
Unsupported local ID Type: <%d>	The phase 1 ID type is not supported by the router.
Build Phase 1 ID	The router has started to build the phase 1 ID.
Adjust TCP MSS to %d	The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel.
Rule <%d> input idle time out, disconnect	The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period.
XAUTH succeed! Username: <Username>	The router used extended authentication to authenticate the listed username.
XAUTH fail! Username: <Username>	The router was not able to use extended authentication to authenticate the listed username.
Rule[%d] Phase 1 negotiation mode mismatch	The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer.
Rule [%d] Phase 1 encryption algorithm mismatch	The listed rule's IKE phase 1 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication algorithm mismatch	The listed rule's IKE phase 1 authentication algorithm did not match between the router and the peer.

Table 131 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Rule [%d] Phase 1 authentication method mismatch	The listed rule's IKE phase 1 authentication method did not match between the router and the peer.
Rule [%d] Phase 1 key group mismatch	The listed rule's IKE phase 1 key group did not match between the router and the peer.
Rule [%d] Phase 2 protocol mismatch	The listed rule's IKE phase 2 protocol did not match between the router and the peer.
Rule [%d] Phase 2 encryption algorithm mismatch	The listed rule's IKE phase 2 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 2 authentication algorithm mismatch	The listed rule's IKE phase 2 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 2 encapsulation mismatch	The listed rule's IKE phase 2 encapsulation did not match between the router and the peer.
Rule [%d]> Phase 2 pfs mismatch	The listed rule's IKE phase 2 perfect forward secret (PFS) setting did not match between the router and the peer.
Rule [%d] Phase 1 ID mismatch	The listed rule's IKE phase 1 ID did not match between the router and the peer.
Rule [%d] Phase 1 hash mismatch	The listed rule's IKE phase 1 hash did not match between the router and the peer.
Rule [%d] Phase 1 preshared key mismatch	The listed rule's IKE phase 1 pre-shared key did not match between the router and the peer.
Rule [%d] Tunnel built successfully	The listed rule's IPSec tunnel has been built successfully.
Rule [%d] Peer's public key not found	The listed rule's IKE phase 1 peer's public key was not found.
Rule [%d] Verify peer's signature failed	The listed rule's IKE phase 1 verification of the peer's signature failed.
Rule [%d] Sending IKE request	IKE sent an IKE request for the listed rule.
Rule [%d] Receiving IKE request	IKE received an IKE request for the listed rule.
Swap rule to rule [%d]	The router changed to using the listed rule.
Rule [%d] Phase 1 key length mismatch	The listed rule's IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer.
Rule [%d] phase 1 mismatch	The listed rule's IKE phase 1 did not match between the router and the peer.
Rule [%d] phase 2 mismatch	The listed rule's IKE phase 2 did not match between the router and the peer.
Rule [%d] Phase 2 key length mismatch	The listed rule's IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer.
Remote Gateway Addr in rule [%s] is changed to %s"	The IP address for the domain name of the peer gateway in the listed rule changed to the listed IP address.
New My ZyWALL Addr in rule [%s] is changed to %s	The IP address for the domain name of the ZyWALL in the listed rule changed to the listed IP address.

Table 131 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Remote Gateway Addr has changed, tunnel [%s] will be deleted	The listed tunnel will be deleted because the remote gateway's IP address changed.
My ZyWALL Addr has changed, tunnel [%s] will be deleted	The listed tunnel will be deleted because the ZyWALL's IP address changed.

Table 132 PKI Logs

LOG MESSAGE	DESCRIPTION
Enrollment successful	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
Enrollment failed	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
Failed to resolve <SCEP CA server url>	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
Enrollment successful	The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port.
Enrollment failed	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
Failed to resolve <CMP CA server url>	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
Rcvd ca cert: <subject name>	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd user cert: <subject name>	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd CRL <size>: <issuer name>	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd ARL <size>: <issuer name>	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ca cert	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received user cert	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received CRL	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ARL	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Rcvd data <size> too large! Max size allowed: <max size>	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.

Table 132 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`Cert trusted: <subject name>`	The router has verified the path of the certificate with the listed subject name.
`Due to <reason codes>, cert not trusted: <subject name>`	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 133 on page 368 for the corresponding descriptions of the codes.

Table 133 Certificate Path Verification Failure Reason Codes

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 134 802.1X Logs

LOG MESSAGE	DESCRIPTION
Local User Database accepts user.	A user was authenticated by the local user database.
Local User Database reports user credential error.	A user was not authenticated by the local user database because of an incorrect user password.
Local User Database does not find user`s credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
Local User Database does not support authentication method.	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
Local User Database does not support authentication mothed.	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use Local User Database to authenticate user.	The local user database is operating as the authentication server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.
No Server to authenticate user.	There is no authentication server to authenticate a user.
Local User Database does not find user`s credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.

Table 135 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.

Table 135 ACL Setting Notes (continued)

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to L/ZW)	LAN to LAN/ ZyWALL	ACL set for packets traveling from the LAN to the LAN or the ZyWALL.
(W to W/ZW)	WAN to WAN/ ZyWALL	ACL set for packets traveling from the WAN to the WAN or the ZyWALL.

Table 136 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message

Table 136 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
16		Information Reply
	0	Information reply message

Table 137 IDP Logs

LOG MESSAGE	DESCRIPTION
The buffer size is too small!	The buffer for holding IDP information such as the signature file version was too small to hold any more information.
The format of the user config file is incorrect!	There was a format error in the configuration backup file that someone attempted to load into the system.
The system is doing signature update now , please wait!	The device is updating the signature file.
No data!	The system could not find any IDP signatures that matched a search.
IDP %s!	The device detected an intrusion event in a connection. The format of %s is “ID” followed by the IDP ID signature number and the IDP signature name. For example, ID:10001,Window Ping.
Can not find the signature , please update the signature!	The device does not have a signature file loaded.
Failed in signature update - %s!	The device failed to update the signature file through the Internet. %s describes the reason for the error. You may need to provide the error message when contacting customer support if you are repeatedly unable to download the signature file from the update server.
Check signature version - %s.	The device attempted to check for the latest available signature version. %s gives details. Either the check was unsuccessful due to the server being busy or the device is already using the latest available firmware.
Signature update OK - New signature version: <Signature version> Release Date: <Release date>!	The device updated the signature file successfully. The signature file’s version and release date are included.

Table 138 AV Logs

LOG MESSAGE	DESCRIPTION
HTTP Virus infected - %s!	The device detected a virus in an HTTP connection. The format of %s is “ID” Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe.
FTPDATA Virus infected - %s!	The device detected a virus in a FTPDATA connection. The format of %s is “ID” Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe.
SMTP Virus infected - %s!	The device detected a virus in a SMTP connection. The format of %s is “ID” Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe.

Table 138 AV Logs (continued)

LOG MESSAGE	DESCRIPTION
POP3 Virus infected - %s!	The device detected a virus in a POP3 connection. The format of %s is "ID" Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe.
HTTP Bypass - %s!	The device bypassed the scanning of files in HTTP connections. %s is the filename. For example, game.zip.
FTPDATA Bypass - %s!	The device bypassed the scanning of files in FTP data connections. %s is the filename. For example, game.zip.
SMTP Bypass - %s!	The device bypassed the scanning of files in SMTP connections. %s is the filename. For example, game.zip.
POP3 Bypass - %s!	The device bypassed the scanning of files in POP3 connections. %s is the filename. For example, game.zip.
Can not find the signature , please update the signature!	The device does not have a signature file loaded.
Failed in signature update - %s!	The device failed to update the signature file through the Internet. %s describes the reason for the error. You may need to provide the error message when contacting customer support if you are repeatedly unable to download the signature file from the update server.
Check signature version - %s.	The device attempted to check for the latest available signature version. %s gives details. Either the check was unsuccessful due to the server being busy or the device is already using the latest available firmware.
Update the signature file successfully.	The device updated the signature file successfully.
The system is doing signature update now , please wait!	The device is updating the signature file.

23.4 Syslog Logs

There are two types of syslog: event logs and traffic logs. The device generates an event log when a system event occurs, for example, when a user logs in or the device is under attack. The device generates a traffic log when a "session" is terminated. A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs.

Table 139 Syslog Logs

LOG MESSAGE	DESCRIPTION
`Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"`	This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. The "devID" is the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.
`Traffic Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="Traffic Log" note="Traffic Log" devID="<mac address>" cat="Traffic Log" duration=seconds sent=sentBytes rcvd=receiveBytes dir="<from:to>" protoID=IPProtocolID proto="serviceName" trans="IPSec/Normal"`	This message is sent by the device when the connection (session) is closed. The facility is defined in the Log Settings screen. The severity is the traffic log type. The message and note always display "Traffic Log". The "proto" field lists the service name. The "dir" field lists the incoming and outgoing interfaces ("LAN:LAN", "LAN:WAN", "LAN:DEV" for example).
`Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"`	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. OB is the Out Break flag and the mac address of the Out Break PC.

Table 139 Syslog Logs (continued)

LOG MESSAGE	DESCRIPTION
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="0|1" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Virus" encode="< uu | b64 >"	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU, LOGS, Log Settings** page. The severity is the log's syslog class. The "encode" message indicates the mail attachments encoding method. The definition of messages and notes are defined in the Anti-Virus log descriptions.
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="IDP" class="<idp class>" sid="<idp sid> act="<idp action>" count="1"	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU, LOGS, Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the IDP log descriptions.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 140 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

24

Maintenance

This chapter displays information on the maintenance screens.

24.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your ZyWALL.

24.2 General Setup and System Name

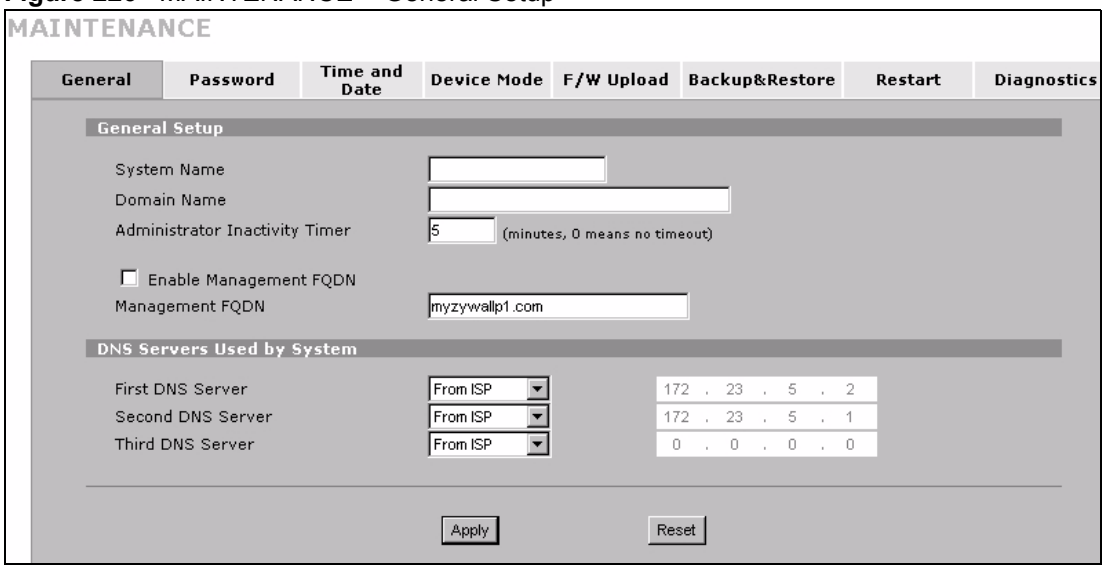
General Setup contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyWALL **System Name**.

24.3 General Setup

Click **MAINTENANCE** to open the **General** screen. Use this screen to configure administrative and system-related information.

Figure 226 MAINTENANCE > General Setup



The following table describes the labels in this screen.

Table 141 MAINTENANCE > General Setup

LABEL	DESCRIPTION
General Setup	
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name), the domain name can be assigned from the ZyWALL via DHCP. Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either through the web configurator or commands) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Enable Management FQDN	Turn on the management FQDN (fully qualified domain name) to use a domain name to access the ZyWALL from the LAN. This allows you to access the ZyWALL without knowing its IP address. The ZyWALL must be in router or zero configuration mode to use the management FQDN to access it.
Management FQDN	Type a fully qualified domain name (FQDN) to use for managing the ZyWALL (www.mydevice.com. for example). An FQDN starts with a host name and continues all the way up to the top-level domain name. In the example, www.mydevice.com, "www" is the host, "mydevice" is the second-level domain, and "com" is the top level domain.

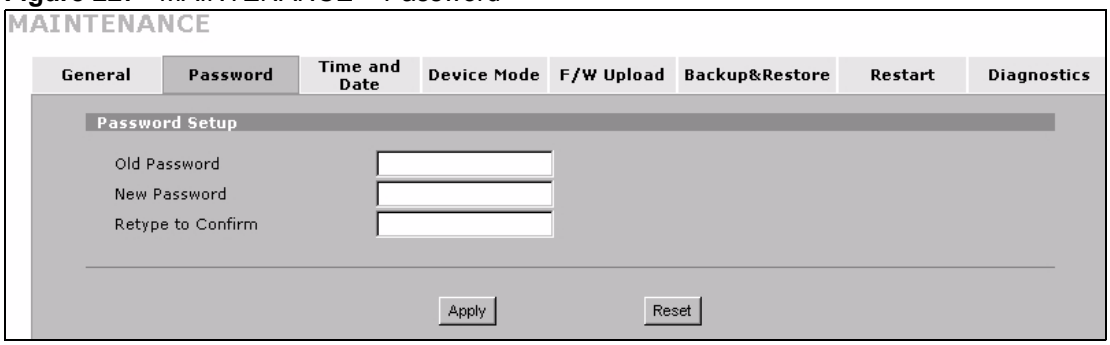
Table 141 MAINTENANCE > General Setup

LABEL	DESCRIPTION
DNS Servers Used by System	The ZyWALL uses these system DNS servers to resolve domain names for features like VPN and updating the time and date from a time server. The following applies when the ZyWALL is in router mode. Select **From ISP** if your ISP dynamically assigns DNS server information. The address field displays the (read-only) DNS server IP address(es) that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. The IP address must be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP addresses of devices in order to access them. In bridge mode, these addresses are all user-defined. Enter the DNS server IP addresses.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

24.4 Configuring Password

Click **MAINTENANCE** > **Password** to open the following screen. Use this screen to change the ZyWALL's management password.

Figure 227 MAINTENANCE > Password



The following table describes the labels in this screen.

Table 142 MAINTENANCE > Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field. If you forget the password, you may have to use the hardware **RESET** button. This restores the default password of 1234.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

24.5 Brute-Force Password Guessing Protection

Brute-force password guessing protection allows you to specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered.

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See Appendix G on page 481 for information on the command structure.

Table 143 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
sys pwderrtm	This command displays the brute-force guessing password protection settings.
sys pwderrtm 0	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
sys pwderrtm N	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

Example

```
sys pwderrtm 5
```

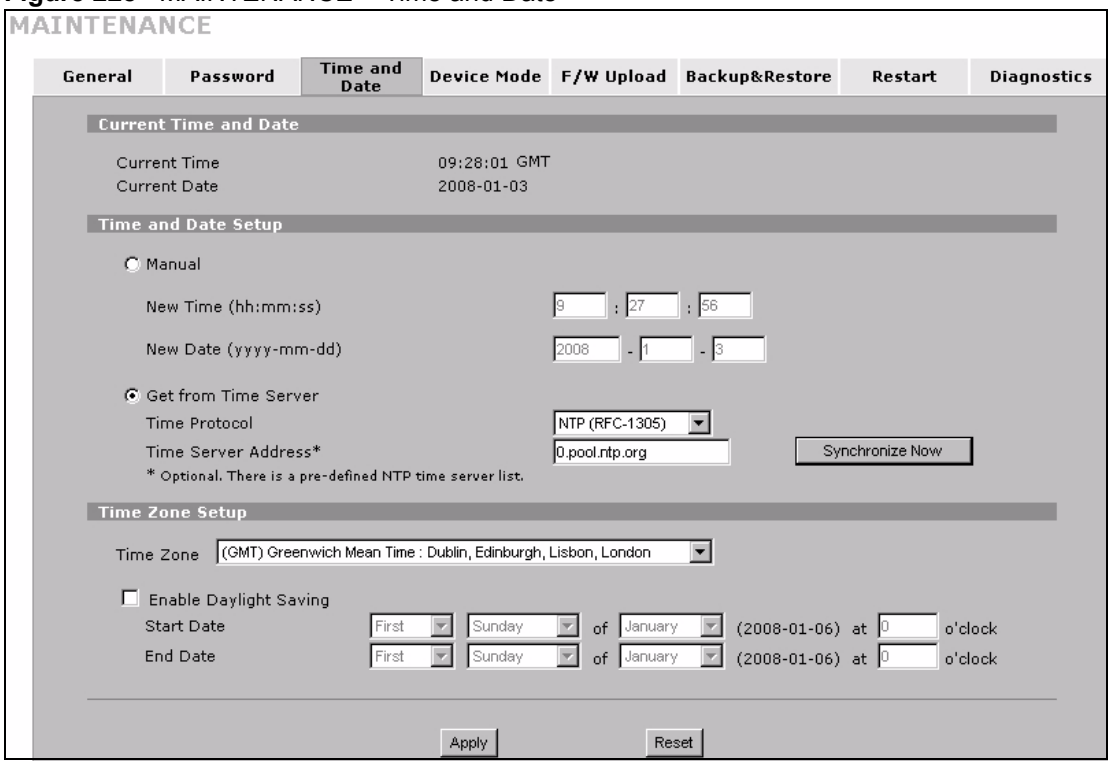
This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

24.6 Time and Date

The ZyWALL's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyWALL.

To change your ZyWALL's time and date, click **MAINTENANCE** > **Time and Date**. The screen appears as shown. Use this screen to configure the ZyWALL's time based on your local time zone.

Figure 228 MAINTENANCE > Time and Date



The following table describes the labels in this screen.

Table 144 MAINTENANCE > Time and Date

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the ZyWALL's present time.
Current Date	This field displays the ZyWALL's present date.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the ZyWALL get the time and date from the time server you specified below.

Table 144 MAINTENANCE > Time and Date (continued)

LABEL	DESCRIPTION
Time Protocol	Select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305)**, is similar to **Time (RFC 868)**.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Synchronize Now	Click this button to have the ZyWALL get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (including the time server address).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **April** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Last**, **Sunday**, **October** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

24.7 Pre-defined NTP Time Server Pools

When you turn on the ZyWALL for the first time, the date and time start at 2000-01-01 00:00:00. The ZyWALL then attempts to synchronize with an NTP time server from one of the 0.pool.ntp.org, 1.pool.ntp.org or 2.pool.ntp.org NTP time server pools. These are virtual clusters of time servers that use a round robin method to provide different NTP servers to clients.

The ZyWALL continues to use the NTP time server pools if you do not specify a time server or it cannot synchronize with the time server you specified.

The ZyWALL can use the NTP time server pools regardless of the time protocol you select.

When the ZyWALL uses the NTP time server pools, it randomly selects one pool and tries to synchronize with a server in it. If the synchronization fails, then the ZyWALL goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time server pools have been tried.

24.7.1 Resetting the Time

The ZyWALL resets the time in the following instances:

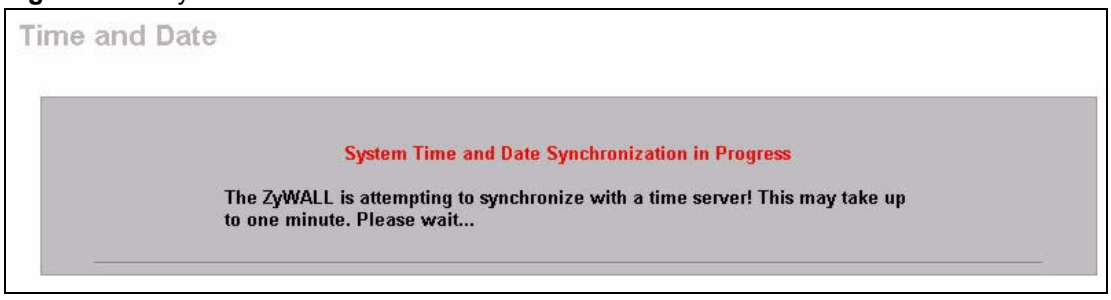
- When you click **Synchronize Now**.
- On saving your changes.
- When the ZyWALL starts up.
- 24-hour intervals after starting.

24.7.2 Time Server Synchronization

Click the **Synchronize Now** button to get the time and date from the predefined time server or the time server you specified in the **Time Server Address** field.

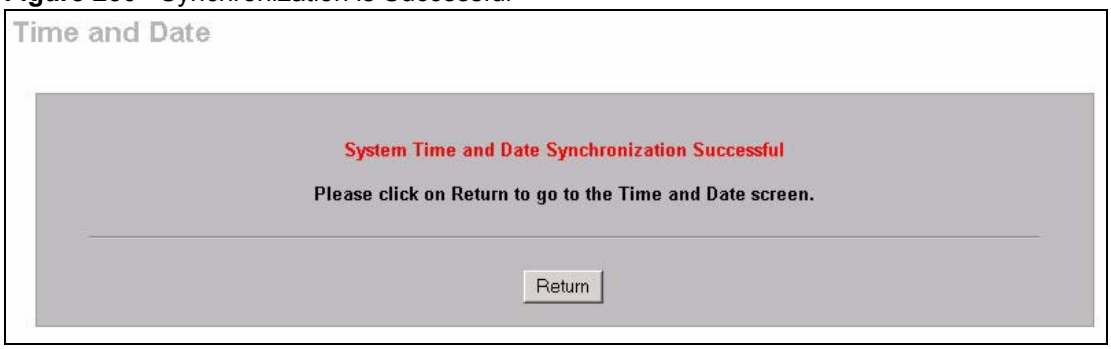
When the **System Time and Date Synchronization in Process** screen appears, wait up to one minute.

Figure 229 Synchronization in Process


Time and Date
System Time and Date Synchronization in Progress
The ZyWALL is attempting to synchronize with a time server! This may take up to one minute. Please wait...

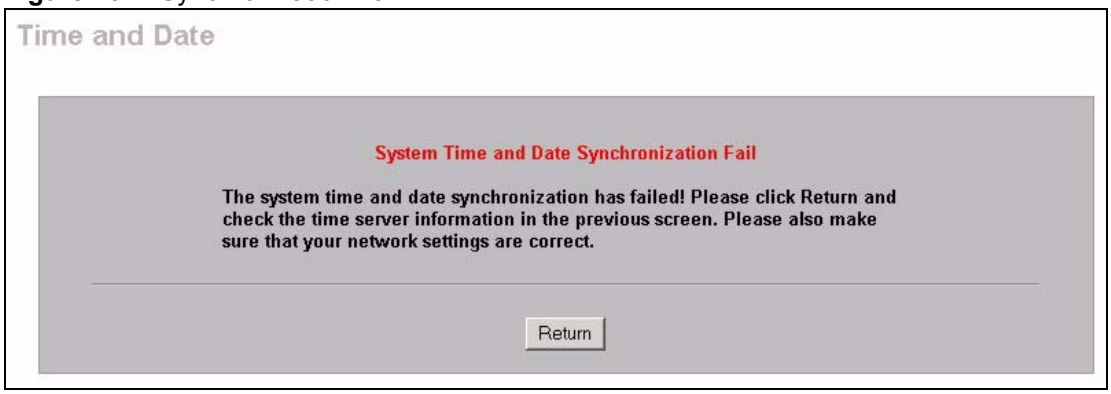
Click the **Return** button to go back to the **Time and Date** screen after the time and date is updated successfully.

Figure 230 Synchronization is Successful


Time and Date
System Time and Date Synchronization Successful
Please click on Return to go to the Time and Date screen.
Return

If the update was not successful, the following screen appears. Click **Return** to go back to the **Time and Date** screen.

Figure 231 Synchronization Fail


Time and Date
System Time and Date Synchronization Fail
The system time and date synchronization has failed! Please click Return and check the time server information in the previous screen. Please also make sure that your network settings are correct.
Return

24.8 Introduction To Transparent Bridging

A transparent bridge is invisible to the operation of a network in that it does not modify the frames it forwards. The bridge checks the source address of incoming frames on the port and learns MAC addresses to associate with that port. All future communications to that MAC address will only be sent on that port.

The bridge gradually builds a host MAC-address-to-port mapping table such as in the following example, during the learning process.

Table 145 MAC-address-to-port Mapping Table

HOST MAC ADDRESS	PORT
00a0c5123456	3
00a0c5123478 (host A)	1
00a0c512349a	3
00a0c51234bc	2
00a0c51234de	4

For example, if a bridge receives a frame via port 1 from host A (MAC address 00a0c5123478), the bridge associates host A with port 1. When the bridge receives another frame on one of its ports with destination address 00a0c5123478, it forwards the frame directly through port 1 after checking the internal table.

The bridge takes one of these actions after it checks the destination address of an incoming frame with its internal table:

- If the table contains an association between the destination address and any of the bridge's ports aside from the one on which the frame was received, the frame is forwarded out the associated port.
- If no association is found, the frame is flooded to all ports except the inbound port. Broadcasts and multicasts also are flooded in this way.
- If the associated port is the same as the incoming port, then the frame is dropped (filtered).

24.9 Transparent Firewalls

A transparent firewall (also known as a in-line, shadow, stealth or bridging firewall) has the following advantages over “router firewalls”:

1. The use of a bridging firewall reduces configuration and deployment time because no networking configuration changes to your existing network (hosts, neighboring routers and the firewall itself) are needed. Just put it in-line with the network it is protecting. As it only moves frames between ports (after inspecting them), it is completely transparent.
2. Performance is improved as there's less processing overhead.
3. As a transparent bridge does not modify the frames it forwards, it is effectively “stealth” as it is invisible to attackers.

Bridging devices are most useful in complex environments that require a rapid or new firewall deployment. A transparent, bridging firewall can also be good for companies with several branch offices since the setups at these offices are often the same and it's likely that one design can be used for many of the networks. A bridging firewall could be configured at HQ, sent to the branches and then installed directly without additional configuration.

24.10 Configuring Device Mode (Router)

Click **MAINTENANCE** > **Device Mode** to open the following screen. Use this screen to have your ZyWALL function as a router, a bridge or a simplified router (zero configuration).

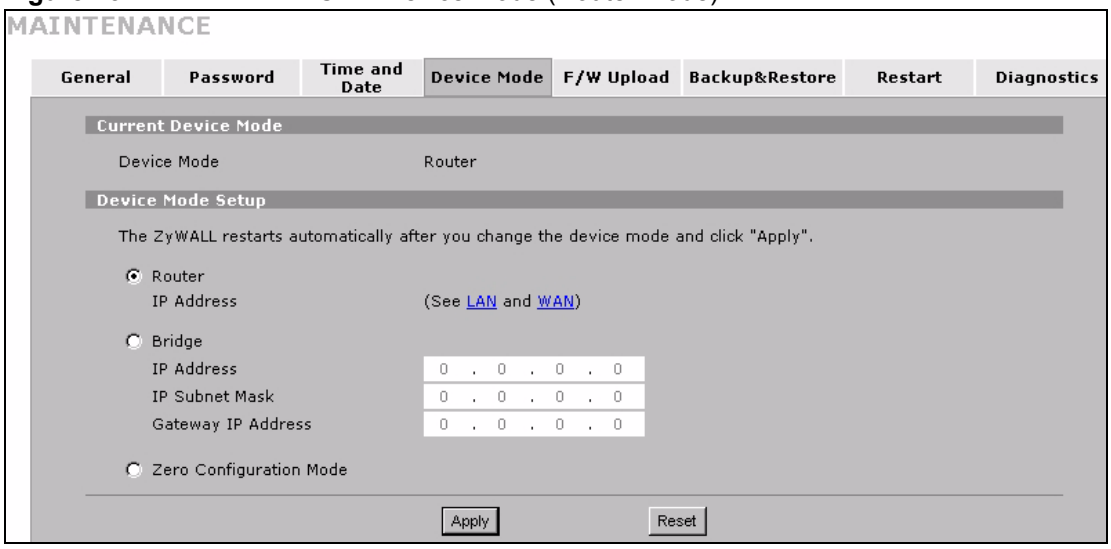
In bridge mode, the ZyWALL functions as a transparent firewall (also known as a bridge firewall). The ZyWALL bridges traffic traveling between the ZyWALL's interfaces and still filters and inspects packets. You do not need to change the configuration of your existing network to use the ZyWALL in bridge mode.

In bridge mode, the ZyWALL cannot get an IP address from a DHCP server. The LAN and WAN interfaces have the same (static) IP address and subnet mask. You can configure the ZyWALL's IP address in order to access the ZyWALL for management. If you connect your computer directly to the ZyWALL, you also need to assign your computer a static IP address in the same subnet as the ZyWALL's IP address in order to access the ZyWALL.

You can use the firewall and VPN in bridge mode. See the user's guide for a list of other features that are available in bridge mode.

The following applies when the ZyWALL is in router mode.

Figure 232 MAINTENANCE > Device Mode (Router Mode)



The following table describes the labels in this screen.

Table 146 MAINTENANCE > Device Mode (Router Mode)

LABEL	DESCRIPTION
Device Mode	This displays whether the ZyWALL is functioning as a router, bridge or simplified router (zero configuration).
Device Mode Setup	
Router	When the ZyWALL is in router mode, there is no need to select or clear this radio button.
IP Address	Click **LAN** or **WAN** to go to the screen where you can view and/or change the corresponding settings.
Bridge	Select this radio button and configure the following fields, then click **Apply** to set the ZyWALL to bridge mode.
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation. Use an IP address in the same subnet as the network to which you connect the ZyWALL. Make sure the IP address does not conflict with any other device on the network.
IP Subnet Mask	Enter the IP subnet mask of the ZyWALL.
Gateway IP Address	Enter the gateway IP address.
Zero Configuration Mode	Use zero configuration mode to have the ZyWALL configure most settings automatically. This is useful for travelers or telecommuters.
Apply	Click **Apply** to save your changes back to the ZyWALL. After you click **Apply**, please wait for one minute and use the IP address you configured in the **IP Address** field to access the ZyWALL again.
Reset	Click **Reset** to begin configuring this screen afresh.

24.11 Configuring Device Mode (Bridge)

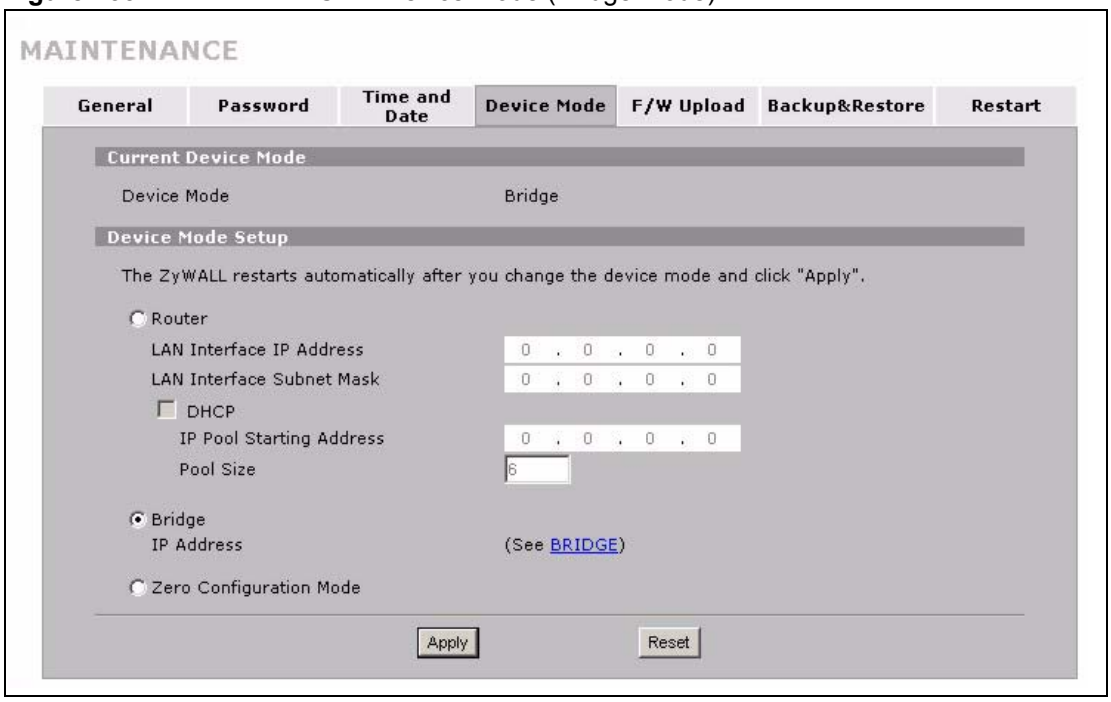
Click **MAINTENANCE** > **Device Mode** to open the following screen. Use this screen to have your ZyWALL function as a router, a bridge or a simplified router (zero configuration).

In bridge mode, the ZyWALL functions as a transparent firewall (also known as a bridge firewall). The ZyWALL bridges traffic traveling between the ZyWALL's interfaces and still filters and inspects packets. You do not need to change the configuration of your existing network.

In bridge mode, the ZyWALL cannot get an IP address from a DHCP server. The LAN and WAN interfaces have the same (static) IP address and subnet mask. You can configure the ZyWALL's IP address in order to access the ZyWALL for management. If you connect your computer directly to the ZyWALL, you also need to assign your computer a static IP address in the same subnet as the ZyWALL's IP address in order to access the ZyWALL.

You can use the firewall and VPN in bridge mode. See the user's guide for a list of other features that are available in bridge mode.

Figure 233 MAINTENANCE > Device Mode (Bridge Mode)



The following table describes the labels in this screen.

Table 147 MAINTENANCE > Device Mode (Bridge Mode)

LABEL	DESCRIPTION
Device Mode	This displays whether the ZyWALL is functioning as a router, bridge or simplified router (zero configuration).
Device Mode Setup	
Router	Select this radio button and click **Apply** to set the ZyWALL to router mode.
LAN Interface IP Address	Enter the IP address of your ZyWALL' s LAN port in dotted decimal notation. 192.168.167.1 is the factory default.

Table 147 MAINTENANCE > Device Mode (Bridge Mode) (continued)

LABEL	DESCRIPTION
LAN Interface Subnet Mask	Enter the IP subnet mask of the ZyWALL's LAN port.
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave the **DHCP** check box selected. Clear it to stop the ZyWALL from acting as a DHCP server. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the rest of the DHCP setup fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
Bridge	When the ZyWALL is in bridge mode, there is no need to select or clear this radio button.
IP Address	Click **Bridge** to go to the **Bridge** screen where you can view and/or change the bridge settings.
Zero Configuration Mode	Use zero configuration mode to have the ZyWALL configure most settings automatically. This is useful for travelers or telecommuters.
Apply	Click **Apply** to save your changes back to the ZyWALL. After you click **Apply**, please wait for one minute and use the IP address you configured in the **LAN Interface IP Address** field to access the ZyWALL again.
Reset	Click **Reset** to begin configuring this screen afresh.

24.12 Configuring Device Mode (Zero Configuration)

Zero configuration mode provides Internet and VPN access for mobile users or telecommuters with little or no configuration. The ZyWALL auto-detects and automatically configures many settings. In zero configuration mode:

- The WAN interface is set to be a DHCP client.
- Auto-detection for DHCP/POE on the WAN interface is enabled.
- IP alias is disabled.
- NAT is set to SUA and full feature NAT is disabled.
- The LAN interface is set to be a DHCP server.
- Network conflict avoidance is enabled.
- The LAN MAC filter is enabled.
- The ZyWALL allows the use of only one VPN network policy. This stops unauthorized use of the other network policies.
- NAT over IPSEC (branch tunnel VPN) is enabled.
- You can use basic **INTERNET ACCESS**, **SECURITY** and **LOGS** screens without logging into the ZyWALL.
- The basic screens let you configure Internet access settings, enable or disable IDP and anti-virus (and update the signatures) and view the logs.
- You must log in to use the advanced screens.

24.12.1 Network Conflict Avoidance

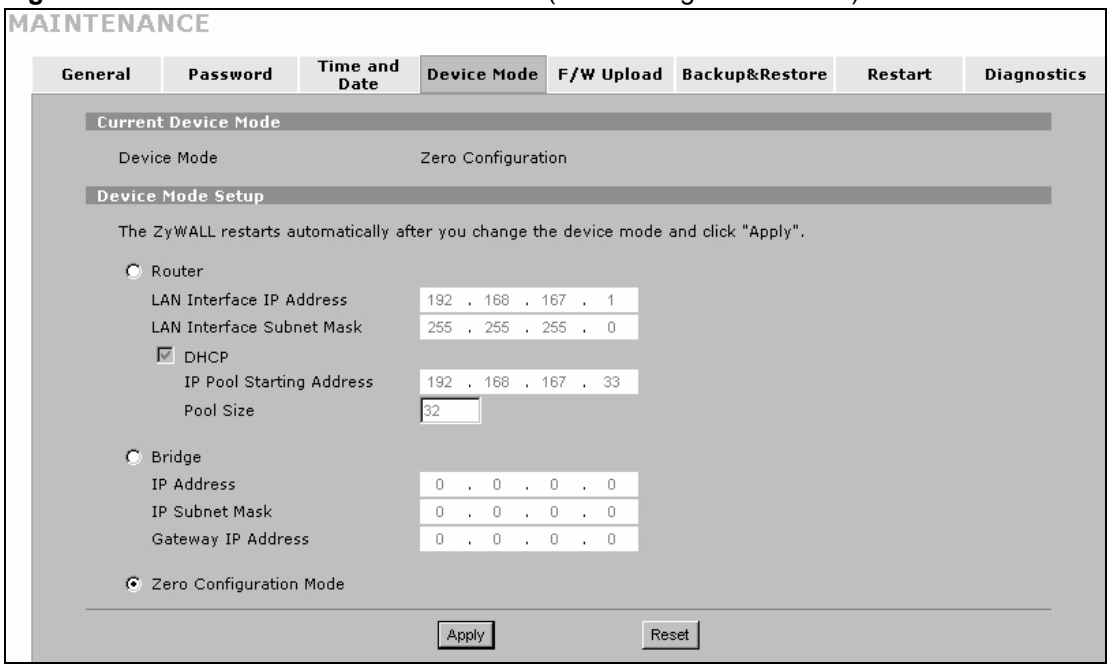
Since your ZyWALL is portable, you may have different WAN interface settings in different locations. In order to avoid network conflicts, the ZyWALL automatically overwrites the following settings if they conflict with the ZyWALL's WAN settings:

- LAN
- LAN DHCP and static DHCP
- IPSec Virtual Address Mapping
- IPSec Port Forwarding Rules

24.13 Configuring Device Mode (Zero Configuration)

Click **MAINTENANCE** > **Device Mode** to open the following screen. Use this screen to have your ZyWALL function as a router, a bridge or a simplified router (zero configuration).

Figure 234 MAINTENANCE > Device Mode (Zero Configuration Mode)



The following table describes the labels in this screen.

Table 148 MAINTENANCE > Device Mode (Zero Configuration Mode)

LABEL	DESCRIPTION
Device Mode	This displays whether the ZyWALL is functioning as a router, bridge or simplified router (zero configuration).
Device Mode Setup	
Router	Select this radio button and click **Apply** to set the ZyWALL to router mode.
LAN Interface IP Address	Enter the IP address of your ZyWALL' s LAN port in dotted decimal notation. 192.168.167.1 is the factory default.
LAN Interface Subnet Mask	Enter the IP subnet mask of the ZyWALL's LAN port.

Table 148 MAINTENANCE > Device Mode (Zero Configuration Mode) (continued)

LABEL	DESCRIPTION
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave the **DHCP** check box selected. Clear it to stop the ZyWALL from acting as a DHCP server. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the rest of the DHCP setup fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
IP Address	Click **Bridge** to go to the **Bridge** screen where you can view and/or change the bridge settings.
Bridge	Select this radio button and configure the following fields, then click **Apply** to set the ZyWALL to bridge mode.
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation.
IP Subnet Mask	Enter the IP subnet mask of the ZyWALL.
Gateway IP Address	Enter the gateway IP address.
Zero Configuration Mode	When the ZyWALL is in zero configuration mode, there is no need to select or clear this radio button.
Apply	Click **Apply** to save your changes back to the ZyWALL. After you click **Apply**, please wait for one minute and use the IP address you configured in the **LAN Interface IP Address** field to access the ZyWALL again.
Reset	Click **Reset** to begin configuring this screen afresh.

24.14 Firmware and Configuration File Maintenance

Use the instructions in the following sections to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Only use firmware for your device's specific model. Refer to the label on the bottom of your ZyWALL.

24.15 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the ZyWALL's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. Find this firmware at www.zyxel.com.With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the ZyWALL.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file "`config.cfg`".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyWALL only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyWALL and the external filename refers to the filename not on the ZyWALL, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **Status** screen to confirm that you have uploaded the correct firmware version.

Table 149 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	rom-0	This is the configuration filename on the ZyWALL. Uploading the rom-0 file replaces the entire ROM file system, including your ZyWALL configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	ras	This is the generic name for the ZyNOS firmware on the ZyWALL.	*.bin

24.16 File Maintenance Over WAN

TFTP, FTP and Telnet over the WAN will not work when:

1. The firewall is active (turn the firewall off or create a firewall rule to allow access from the WAN).
2. You have disabled the service in the remote management screens (see Chapter 18 on page 297).
3. The IP you entered in the **Secure Client IP** field in the remote management screens does not match the client IP. The ZyWALL disconnects the session immediately if it does not match (see Chapter 18 on page 297).

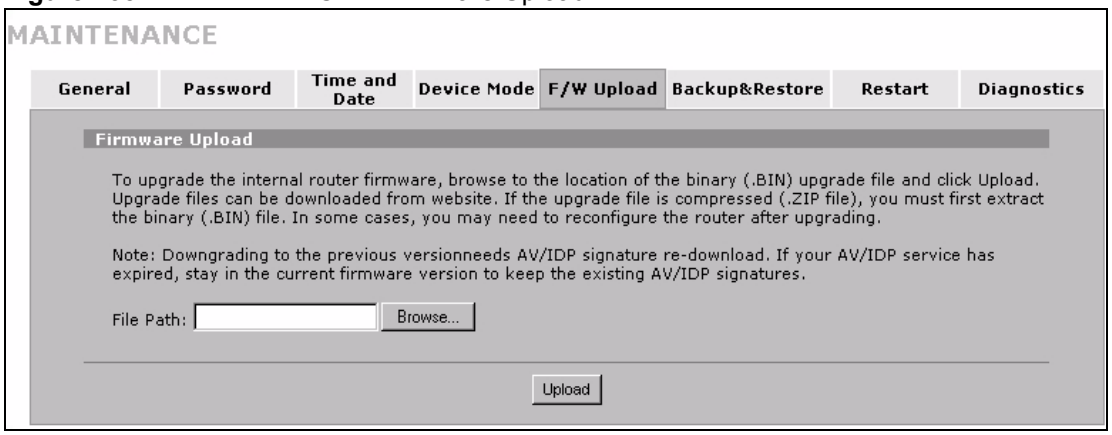
24.17 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "zywall.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Section 24.21 on page 397 for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE** > **F/W UPLOAD**. Follow the instructions in this screen to upload firmware to your ZyWALL.

Only upload firmware for your specific model!

Figure 235 MAINTENANCE > Firmware Upload


MAINTENANCE
General
Password
Time and Date
Device Mode
F/W Upload
Backup&Restore
Restart
Diagnostics
Firmware Upload
To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure the router after upgrading.
Note: Downgrading to the previous versionneeds AV/IDP signature re-download. If your AV/IDP service has expired, stay in the current firmware version to keep the existing AV/IDP signatures.
File Path:
Browse...
Upload

The following table describes the labels in this screen.

Table 150 MAINTENANCE > Firmware Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Do not turn off the ZyWALL while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyWALL again.

Figure 236 Firmware Upload In Process

FIRMWARE UPLOAD
Firmware Upload In Progress
Warning!
Do Not Turn Off the Device.
Please wait for the device to finish restarting. After the device finishes rebooting, the login screen displays.
To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status screen.

The ZyWALL automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 237 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **HOME** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

Figure 238 Firmware Upload Error

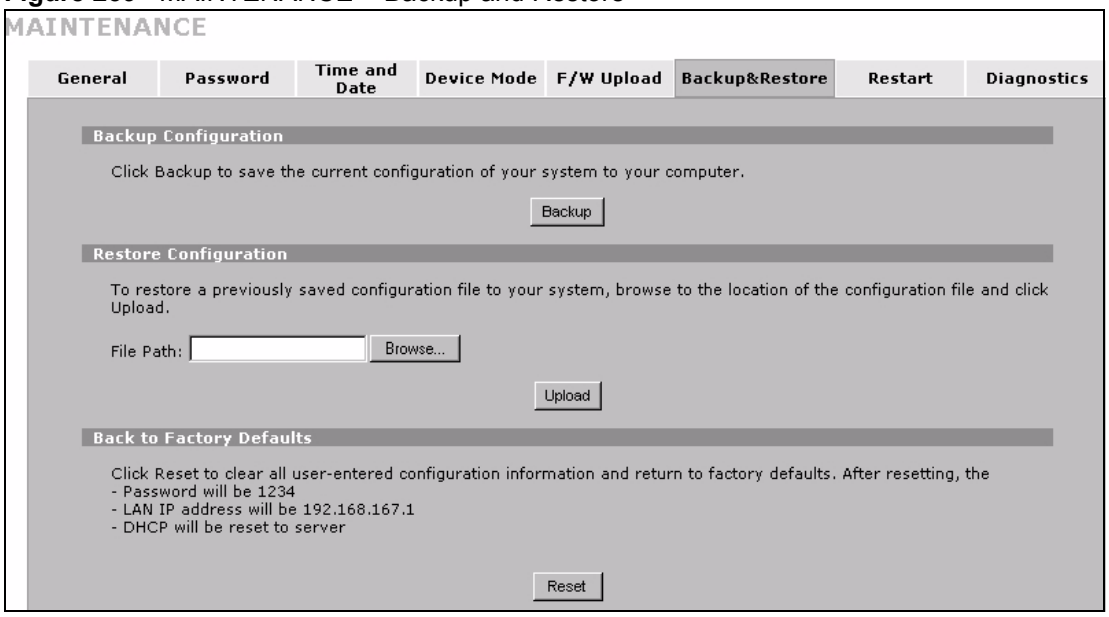
FIRMWARE UPLOAD
Firmware upload error!
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.
Return

24.18 Backup and Restore

See later in this chapter for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE** > **Backup & Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 239 MAINTENANCE > Backup and Restore


MAINTENANCE
General
Password
Time and Date
Device Mode
F/W Upload
Backup&Restore
Restart
Diagnostics
Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
File Path:
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.167.1
- DHCP will be reset to server
Reset

24.18.1 Backup Configuration

Backup configuration allows you to back up (save) the ZyWALL's current configuration to a file on your computer. Once your ZyWALL is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyWALL's current configuration to your computer.

24.18.2 Restore Configuration

Load a configuration file from your computer to your ZyWALL.

Table 151 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Do not turn off the ZyWALL while configuration file upload is in progress.

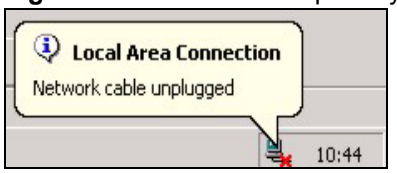
After you see a "restore configuration successful" screen, you must then wait one minute before logging into the ZyWALL again.

Figure 240 Configuration Upload Successful

RESTORE CONFIGURATION
Restore Configuration Successful
The Router Is Rebooting Now.
Please Wait ...
After the device finishes rebooting, the login screen displays.

The ZyWALL automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 241 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.167.1). See your Quick Start Guide for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

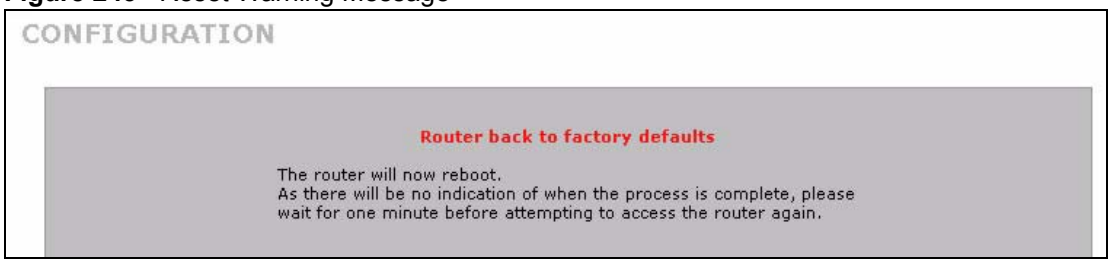
Figure 242 Configuration Upload Error

RESTORE CONFIGURATION
Restore configuration error!
The configuration file was not accepted by the router. Please return to the previous page and select a valid configuration file. Click Help for more information.
Return

24.18.3 Back to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the ZyWALL to its factory defaults as shown on the screen. The following warning screen appears.

Figure 243 Reset Warning Message


CONFIGURATION
Router back to factory defaults
The router will now reboot.
As there will be no indication of when the process is complete, please
wait for one minute before attempting to access the router again.

You can also press the hardware **RESET** button to reset the factory defaults of your ZyWALL. Refer to Section 26.6 on page 425 for more information on the **RESET** button.

24.19 Using FTP or TFTP to Back Up Configuration

This section covers how to use FTP or TFTP to save your ZyWALL's configuration file to your computer.

24.19.1 Using the FTP Commands to Back Up Configuration

1. Launch the FTP client on your computer.
2. Enter "`open`", followed by a space and the IP address of your ZyWALL.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "1234").
5. Enter "`bin`" to set transfer mode to binary.
6. Use "`get`" to transfer files from the ZyWALL to the computer, for example, "`get rom-0 config.rom`" transfers the configuration file on the ZyWALL to your computer and renames it "`config.rom`". See earlier in this chapter for more information on filename conventions.
7. Enter "`quit`" to exit the ftp prompt.

24.19.2 FTP Command Configuration Backup Example

This figure gives an example of using FTP commands from the DOS command prompt to save your ZyWALL's configuration onto your computer.

Figure 244 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

24.19.3 Configuration Backup Using GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 152 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

24.19.4 Backup Configuration Using TFTP

The ZyWALL supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Enter command "`sys stdio 0`" to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter command "`sys stdio 5`" to restore the five-minute management idle timeout (default) when the file transfer is complete.
3. Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.
4. Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the configuration file is "`rom-0`" (rom-zero, not capital o).

Note that the telnet connection must be active before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "`get`" to transfer from the ZyWALL to the computer and "binary" to set binary transfer mode.

24.19.5 TFTP Command Configuration Backup Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the ZyWALL IP address, "get" transfers the file source on the ZyWALL (rom-0, name of the configuration file on the ZyWALL) to the file destination on the computer and renames it config.rom.

24.19.6 Configuration Backup Using GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 153 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyWALL. 192.168.167.1 is the ZyWALL's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the ZyWALL and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyWALL. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to Section 24.16 on page 389 to read about configurations that disallow TFTP and FTP over WAN.

24.20 Using FTP or TFTP to Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR device. When the restore configuration process is complete, the device will automatically restart.

24.20.1 Restore Using FTP Session Example

Figure 245 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to Section 24.16 on page 389 to read about configurations that disallow TFTP and FTP over WAN.

24.21 FTP and TFTP Firmware and Configuration File Uploads

This section shows you how to upload firmware and configuration files.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR device.

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client. The following sections give examples of how to upload the firmware and the configuration files.

24.21.1 FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your ZyWALL.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Use “put” to transfer files from the computer to the ZyWALL, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the ZyWALL and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyWALL to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.

24.21.2 FTP Session Example of Firmware File Upload

Figure 246 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to the File Maintenance Over WAN section to read about configurations that disallow TFTP and FTP over WAN.

24.21.3 TFTP File Upload

The device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. Do the following to transfer the firmware and the configuration file.

1. Use telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Enter the command “sys stdio 0” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute management idle timeout (default) when the file transfer is complete.
3. Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.
4. Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the ZyWALL in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyWALL to the computer, “put” the other way around, and “binary” to set binary transfer mode.

24.21.4 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyWALL’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyWALL).

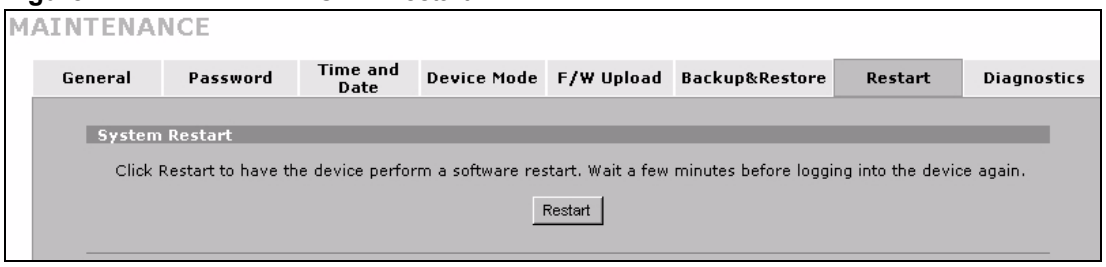
Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

24.22 Restart Screen

System restart allows you to reboot the ZyWALL without turning the power off.

Click **MAINTENANCE** > **Restart**. Click **Restart** to have the ZyWALL reboot. Restart is different to reset; (see Section 24.18.3 on page 393) reset returns the device to its default configuration.

Figure 247 MAINTENANCE > Restart



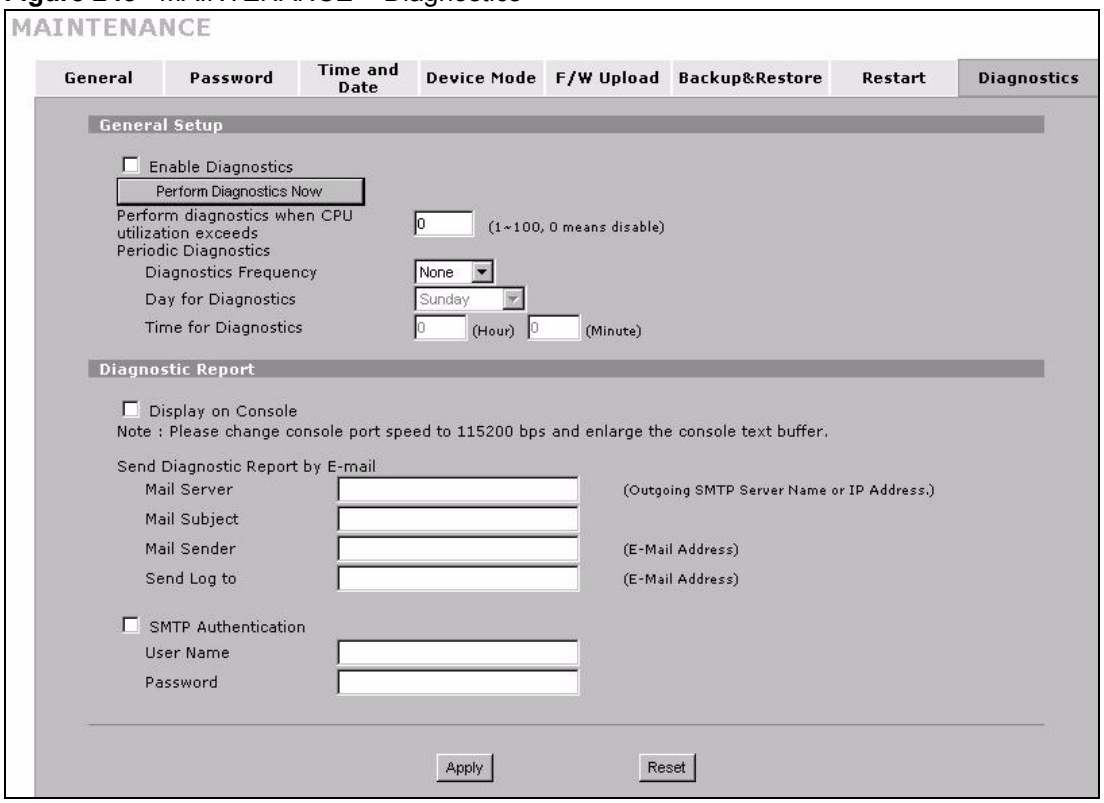
24.23 Diagnostics

Use the **Diagnostics** screen to have the ZyWALL generate and send diagnostic files by e-mail and/or the console port. The diagnostics files contain the ZyWALL’s configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

Click **MAINTENANCE > Diagnostics** to open the following screen.

The ZyWALL sends only one diagnostic e-mail within five minutes (unless you click **Perform Diagnostics Now**).

Figure 248 MAINTENANCE > Diagnostics



The following table describes the labels in this screen.

Table 154 MAINTENANCE > Diagnostics

LABEL	DESCRIPTION
Enable Diagnostics	Select this option to turn on the diagnostics feature.
Perform Diagnostics when CPU utilization exceeds	Set the ZyWALL to generate and send a diagnostic file every time the CPU usage exceeds the specified percent for more than 60 seconds. Enter 0 to have the ZyWALL not generate and send diagnostic files based on CPU usage going over a specific level.
Display on Console	Select this option to have the ZyWALL send diagnostic information through the console port. To receive the information through the console port, you still need to configure the mail settings and open a terminal emulation program on the computer connected to the console port. To handle the size of the diagnostic file, change your console port speed to 115200 bps (on both the ZyWALL and your terminal emulation program) and enlarge the console text buffer.
E-mail Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail address specified in the **Mail Sender** field. If this field is left blank, diagnostic files will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the diagnostic e-mail message that the ZyWALL sends.
Mail Sender	Enter the e-mail address that you want to be in the from/sender line of the diagnostic e-mail message that the ZyWALL sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well.
Send Report to	Diagnostic files are sent to the e-mail address specified in this field. If this field is left blank, diagnostic files will not be sent via e-mail.

Table 154 MAINTENANCE > Diagnostics (continued)

LABEL	DESCRIPTION
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the diagnostic files.
User Name	Enter the user name (up to 63 characters) (usually the user name of a mail account you specified in the **Mail Sender** field).
Password	Enter the password associated with the user name above.
Perform Diagnostics Now	Click this button to generate and send a diagnostic file immediately, instead of based on a time period or CPU usage level.
Schedule	
Periodic Diagnostics	Use these fields to set the ZyWALL to generate and send diagnostic files at regular intervals. Even if you enable both CPU utilization-based and periodic diagnosis, the ZyWALL only sends one diagnostic file within five minutes (unless you click **Perform Diagnostics Now**).
Diagnostics Frequency	Set how often the ZyWALL generates and sends diagnostic files. **Hourly** **Daily** **Weekly** **None**. If you select **Daily** or **Weekly**, specify a time of day for the ZyWALL to generate and send diagnostic files. If you select **Weekly**, then also specify which day of the week. Select **None** to have the ZyWALL not generate and send diagnostic files based on a time period.
Day for Diagnostics	Use the drop down list box to select which day of the week to generate and send diagnostic files.
Time for Diagnostics	Enter the time of day in 24-hour format (for example 23:00 equals 11:00 pm) to generate and send diagnostic files.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

PART VI
Zero Configuration

Zero Configuration Screens (405)

25

Zero Configuration Screens

25.1 Overview

This chapter describes the ZyWALL's zero configuration web configurator screens.

In zero configuration mode, you can use some web configurator screens without logging in with the administrator password. Use the following process to access the web configurator when the ZyWALL is in zero configuration mode. See Section 2.2 on page 43 for how to log into the web configurator when the ZyWALL is in router or bridge mode.

1. Make sure your ZyWALL hardware is properly connected and prepare your computer/ computer network to connect to the ZyWALL (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type the ZyWALL's IP address as the URL ("192.168.167.1" is the default). Alternatively, if you have enabled the management FQDN (Fully Qualified Domain Name), you can use the management domain name to access the ZyWALL from the LAN (see Section 24.3 on page 375 for details).

Figure 249 Zero Configuration

25.1.1 What You Can Do in the Zero Configuration Screens

Use the **Internet Access** screen (Section 25.2 on page 406) to see general network status information and configure the Internet access settings.

Use the **VPN** screen (Section 25.3 on page 412) to establish a VPN connection.

Use the **SA Monitor** screen (Section 25.3.2 on page 413) to display and manage active VPN connections.

Use the **Security** screen (Section 25.4 on page 414) to enable or disable the ZyWALL's IDP and anti-virus features and update the IDP signatures and anti-virus patterns file.

Use the **Logs** screen (Section 25.5 on page 415) to display the ZyWALL's logs.

Advanced: Click this link to go to the advanced configuration area.

Exit: Click this link to exit the Zero Configuration screen.

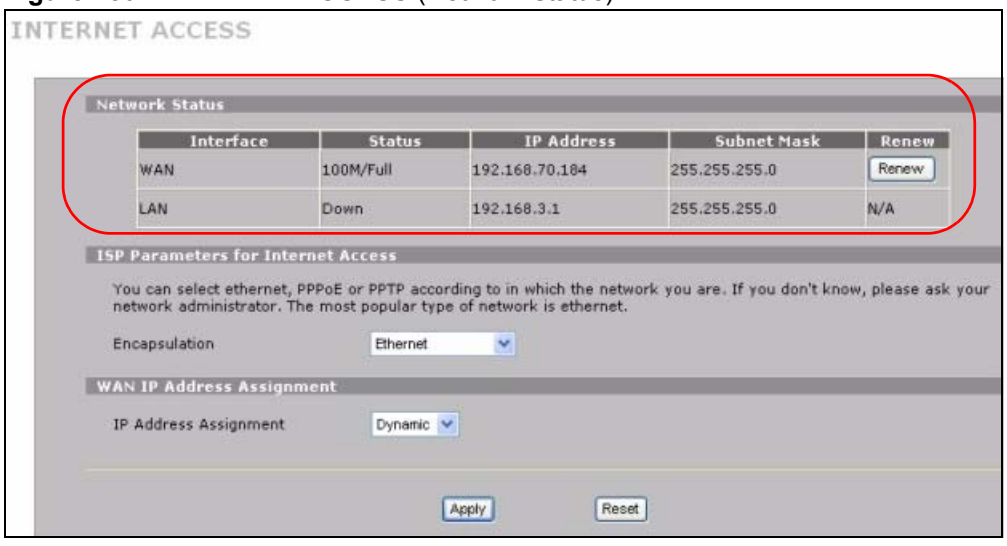
25.2 The Internet Access Screen

The **INTERNET ACCESS** screen displays when the ZyWALL is set to zero configuration mode. This screen displays general network status information about the ZyWALL and allows you to configure the Internet access settings.

25.2.1 Network Status

The first part of this screen displays general network status information about the ZyWALL.

Figure 250 INTERNET ACCESS (Network Status)



The following table describes the **Network Status** labels in this screen.

Table 155 INTERNET ACCESS (Network Status)

LABEL	DESCRIPTION
Interface	This is the port type.
Status	For the LAN port, this displays the port speed and duplex setting. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect. For the WAN port the port speed and duplex setting display if you're using Ethernet encapsulation and **Down** (line is down or not connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you're using PPPoE encapsulation.
IP Address	This shows the port's IP address.
Subnet Mask	This shows the port's subnet mask.
Renew	If you are using Ethernet encapsulation and the WAN port is configured to get the IP address automatically from the ISP, click **Renew** to release the WAN port's dynamically assigned IP address and get the IP address afresh.

25.2.2 ISP Parameters

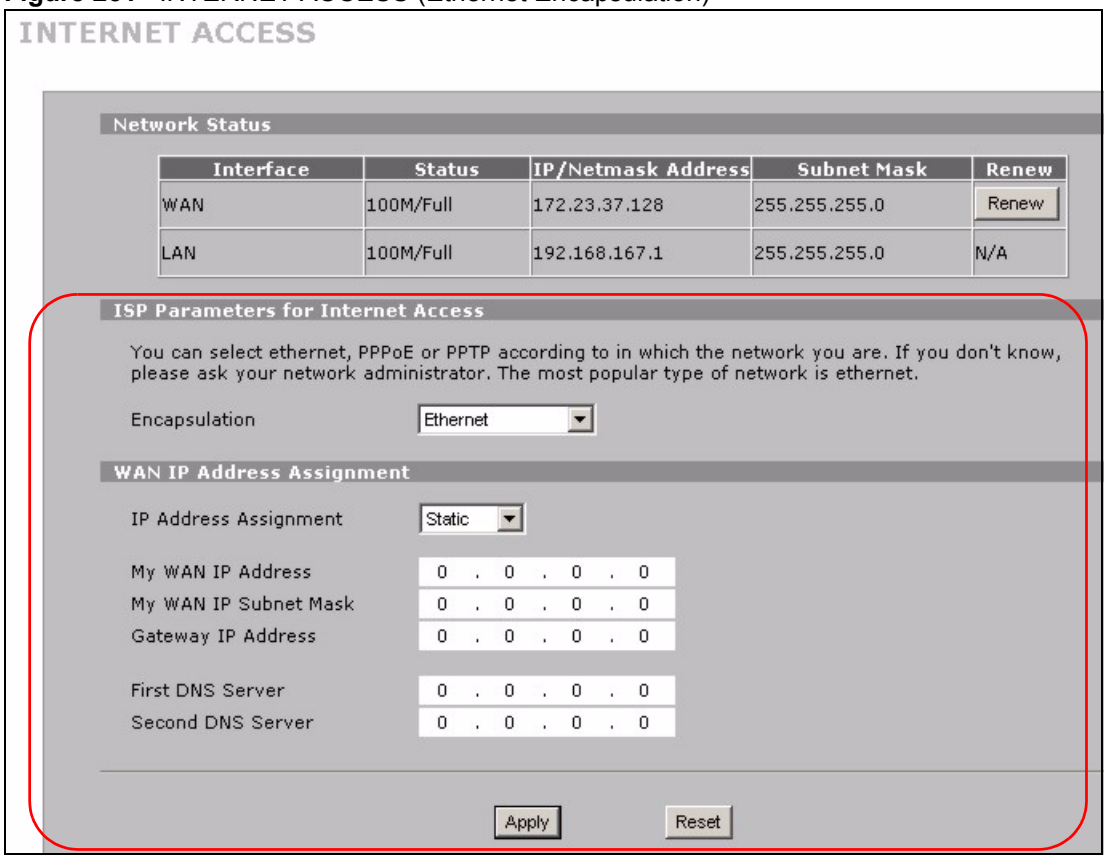
The ZyWALL offers **Ethernet**, **PPTP** and **PPPoE** choices for encapsulation. The screen varies depending on what encapsulation type you use. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

25.2.2.1 Ethernet

For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a **WAN-to-WAN/ZyWALL** firewall rule for those packets. Contact your ISP to find the correct port number.

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

Figure 251 INTERNET ACCESS (Ethernet Encapsulation)



The following table describes the Internet access configuration labels in this screen.

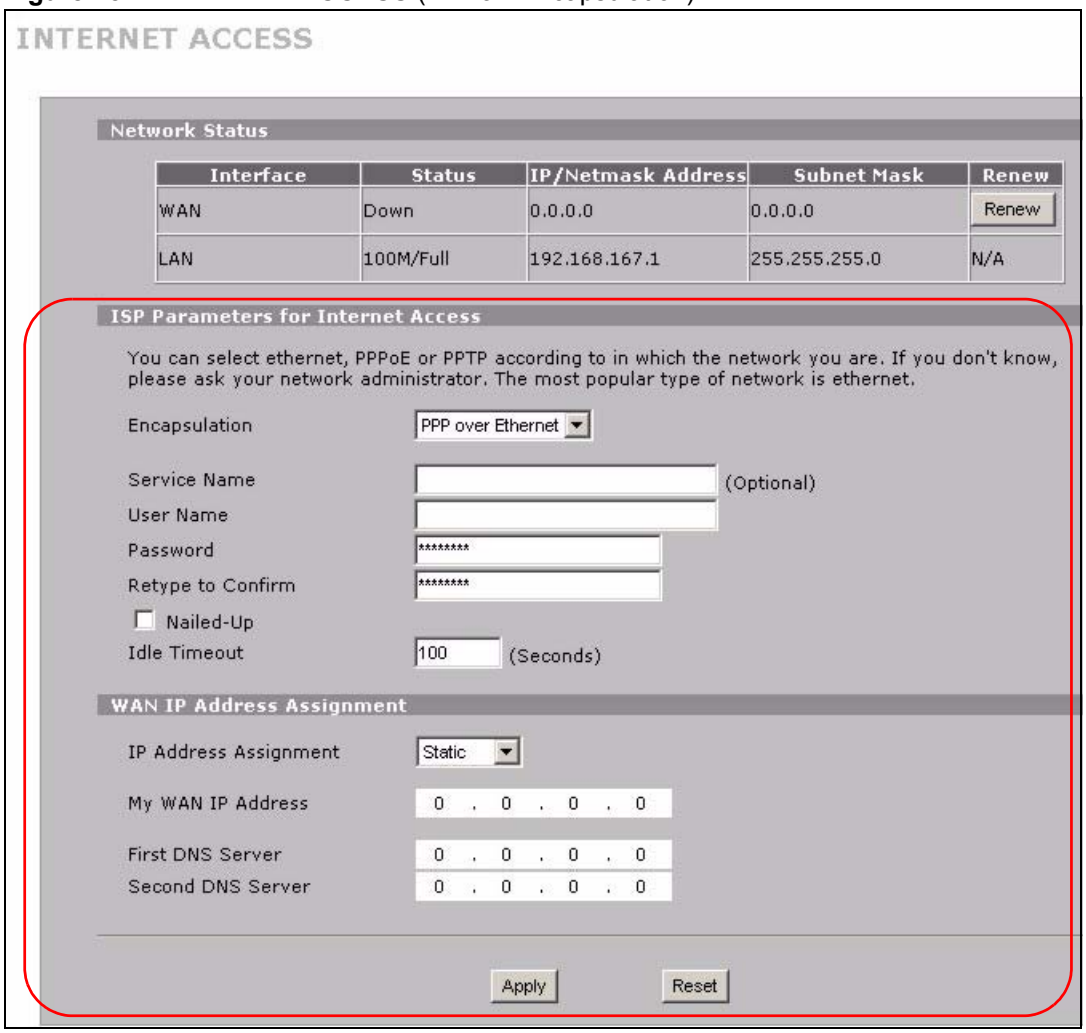
Table 156 INTERNET ACCESS (Ethernet Encapsulation)

LABEL	DESCRIPTION
Encapsulation	You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection.
WAN IP Address Assignment	
IP Address Assignment	Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection. Select **Static** If the ISP assigned a fixed IP address. The fields below are available only when you select **Static**.
My WAN IP Address	Enter your WAN IP address in this field.
My WAN IP Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address	Enter the gateway IP address in this field.
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

25.2.2.2 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

Figure 252 INTERNET ACCESS (PPPoE Encapsulation)



The following table describes the Internet access configuration labels in this screen.

Table 157 INTERNET ACCESS (PPPoE Encapsulation)

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Encapsulation	Choose an encapsulation method from the pull-down list box. **PPP over Ethernet** forms a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.

Table 157 INTERNET ACCESS (PPPoE Encapsulation) (continued)

LABEL	DESCRIPTION
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is **100** seconds.
WAN IP Address Assignment	
IP Address Assignment	Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection. Select **Static** If the ISP assigned a fixed IP address. The fields below are available only when you select **Static**.
My WAN IP Address	Enter your WAN IP address in this field.
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

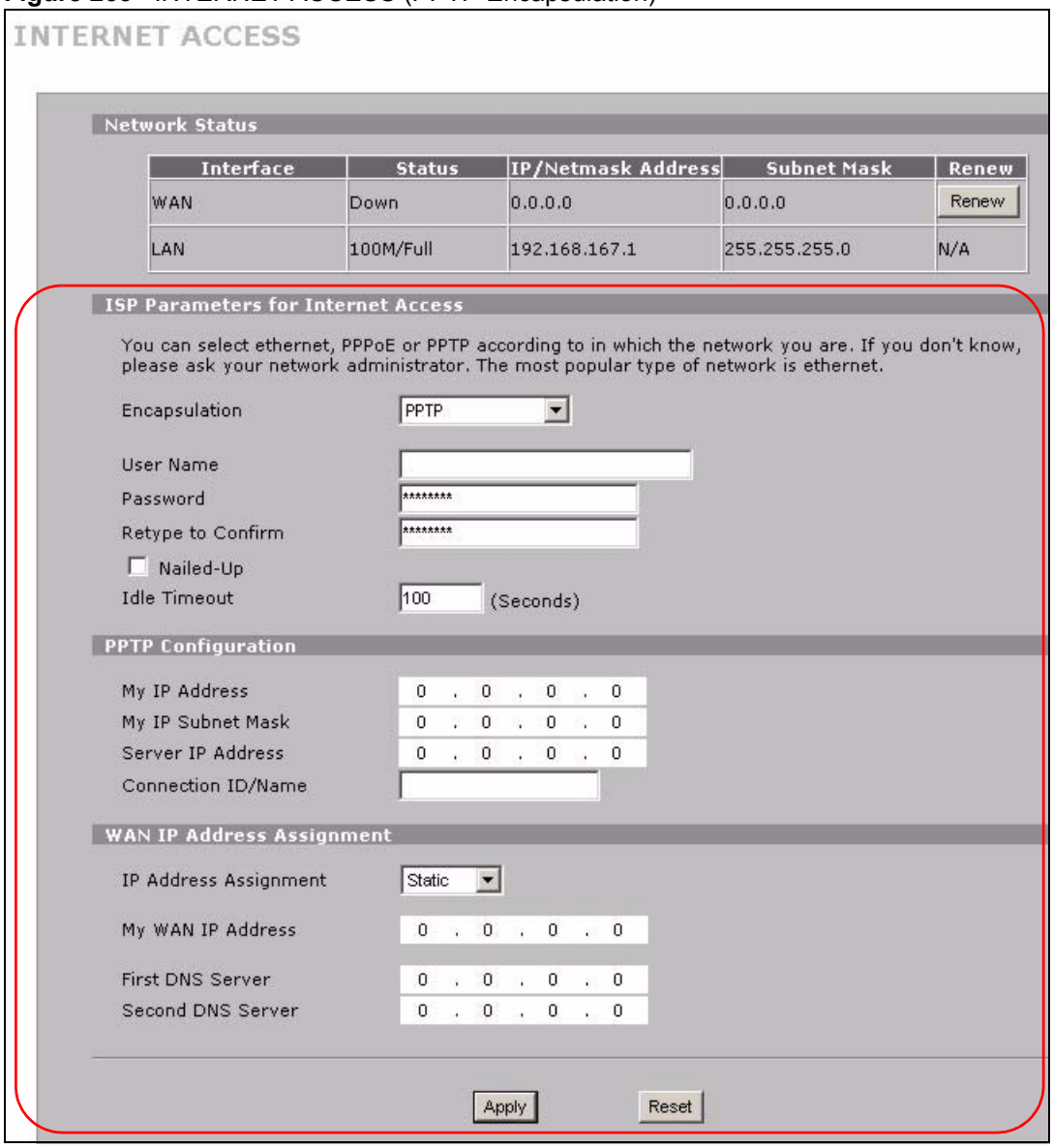
25.2.2.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

The ZyWALL supports one PPTP server connection at any given time.

Figure 253 INTERNET ACCESS (PPTP Encapsulation)



The following table describes the Internet access configuration labels in this screen.

Table 158 INTERNET ACCESS (PPTP Encapsulation)

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select **PPTP** from the drop-down list box. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.

Table 158 INTERNET ACCESS (PPTP Encapsulation)

LABEL	DESCRIPTION
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your DSL modem.
WAN IP Address Assignment	
IP Address Assignment	Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection. Select **Static** If the ISP assigned a fixed IP address. The fields below are available only when you select **Static**.
My WAN IP Address	Enter your WAN IP address in this field.
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

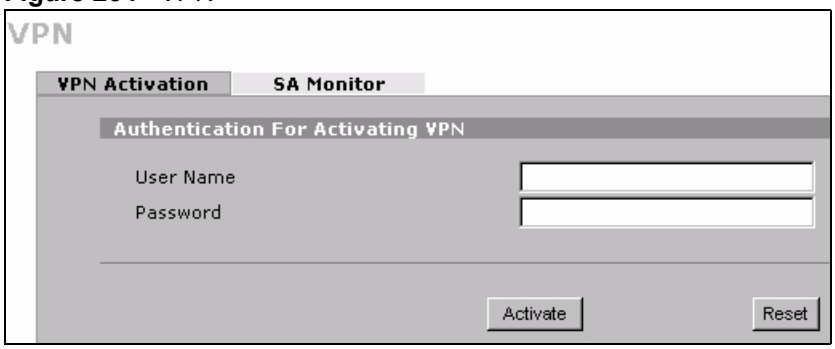
25.3 The VPN Screen

Use this screen to establish a VPN connection using an already configured and activated VPN rule. The **VPN** screens are only available when a VPN rule is activated. See Chapter 13 on page 203 for more information on configuring a VPN rule.

25.3.1 VPN Activation

Activate your VPN connection by entering the username and password information that has been provided to you. Click **Activate** after entering your details to try and establish a VPN connection to a remote network. Click **Reset** to clear the fields.

Figure 254 VPN



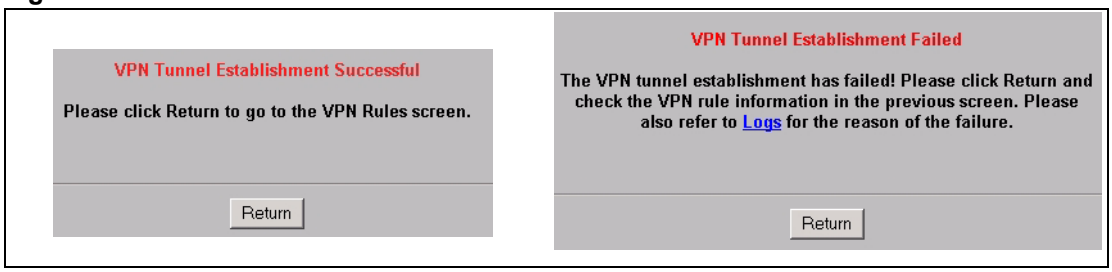
The following table describes the labels in this screen.

Table 159 VPN Activation

LABEL	DESCRIPTION
User Name	Enter into the field the User Name provided to you for your VPN connection.
Password	Enter into the field the password provided to you for your VPN connection.
Activate	Click **Activate** after entering your user details to try and establish a VPN connection.
Reset	Click **Reset** to clear the User Name and Password fields.

When the ZyWALL has a successful VPN connection to the remote network, click **Return** to display the main VPN screen. If the VPN connection fails, click **Return** and make sure the VPN rule is configured correctly in the web configurator and that you have internet access.

Figure 255 VPN

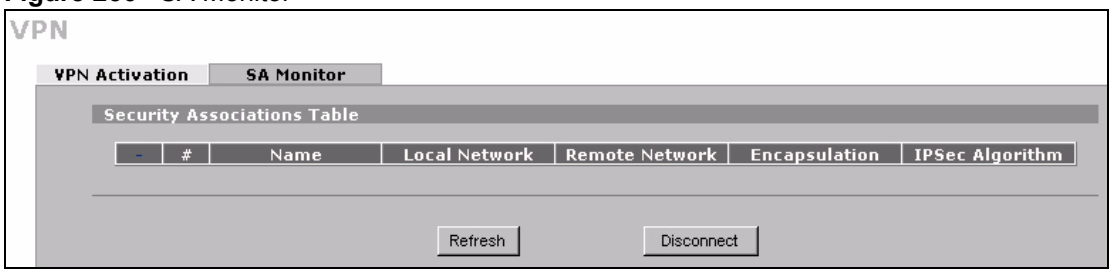

VPN Tunnel Establishment Successful
Please click Return to go to the VPN Rules screen.
Return
VPN Tunnel Establishment Failed
The VPN tunnel establishment has failed! Please click Return and check the VPN rule information in the previous screen. Please also refer to Logs for the reason of the failure.
Return

25.3.2 The SA Monitor Screen

Click **VPN > SA Monitor** to access this screen. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections.

Figure 256 SA Monitor



The following table describes the labels in this screen.

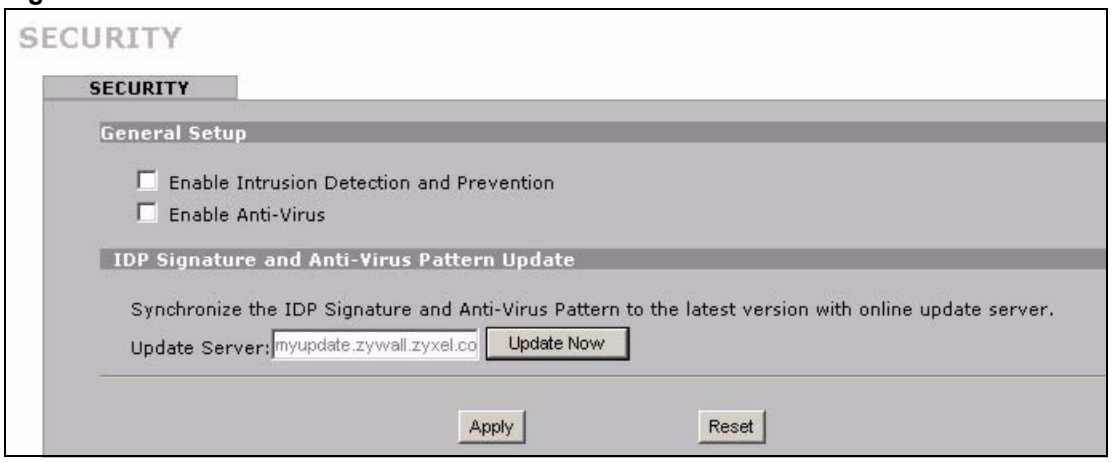
Table 160 SA Monitor

LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Local Network	This field displays the IP address of the computer using the VPN IPSec feature of your ZyWALL.
Remote Network	This field displays IP address (in a range) of computers on the remote network behind the remote IPSec router.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase ZyWALL processing requirements and communications latency (delay).
Refresh	Click **Refresh** to display the current active VPN connection(s).
Disconnect	Select a security association index number that you want to disconnect and then click **Disconnect**.

25.4 The Security Screen

Click **SECURITY** to display this screen. Use this screen to enable or disable the ZyWALL's IDP and anti-virus features and update the IDP signatures and anti-virus patterns file.

Figure 257 SECURITY



The following table describes the labels in this screen.

Table 161 SECURITY

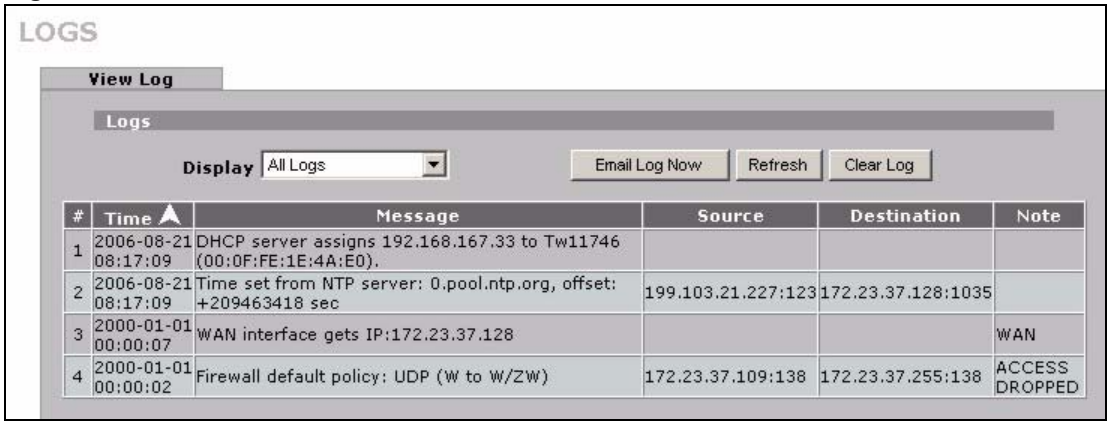
LABEL	DESCRIPTION
General Setup	
Enable Intrusion Detection and Protection	Select this check box to enable IDP on the ZyWALL. When this check box is cleared the ZyWALL is in IDP “bypass” mode and no IDP checking is done.
Enable Anti-Virus	Select this check box to check traffic for viruses. The anti-virus scanner works on the following. FTP traffic using TCP ports 20 and 21 HTTP traffic using TCP ports 80, 8080 and 3128 POP3 traffic using TCP port 110 SMTP traffic using TCP port 25
IDP Signature and Anti Virus Pattern Update	
Update Server	This is the URL of the server from which you download the signatures and pattern file.
Update Now	Click this button to download the signature and pattern file from the **Update Server** immediately.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

25.5 The Logs Screen

Click **LOGS** to display this screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (you must log into the web configurator to access the **Log Settings** screen). See Chapter 23 on page 351 for more information on the logs and selecting categories of logs for the ZyWALL to collect.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 258 LOGS


LOGS
View Log
Logs
Display
All Logs
Email Log Now
Refresh
Clear Log
Time Message Source Destination Note
1 2006-08-21 08:17:09 DHCP server assigns 192.168.167.33 to Tw11746 (00:0F:FE:1E:4A:E0).
2 2006-08-21 08:17:09 Time set from NTP server: 0.pool.ntp.org, offset: +209463418 sec 199.103.21.227:123 172.23.37.128:1035
3 2000-01-01 00:00:07 WAN interface gets IP:172.23.37.128 WAN
4 2000-01-01 00:00:02 Firewall default policy: UDP (W to W/ZW) 172.23.37.109:138 172.23.37.255:138 ACCESS DROPPED

The following table describes the labels in this screen.

Table 162 LOGS

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** page (see Section 23.3 on page 353) display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Log Settings**, see Section 23.3 on page 353).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.
#	This field displays the log number.
Time	This field displays the time the log was recorded. See Section 24.6 on page 378 to configure the ZyWALL's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.

PART VII
Troubleshooting and Specifications

Troubleshooting (419)
Product Specifications (427)

26

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyWALL Access and Login
- Internet Access
- VoIP
- Advanced Features

26.1 Power, Hardware Connections, and LEDs

The ZyWALL does not turn on. None of the LEDs turn on.

1. Make sure you are using the included USB cable or the appropriate power adaptor for the ZyWALL.
2. Make sure the USB cable power adaptor is connected to the ZyWALL and plugged in to an appropriate USB port or power outlet. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the ZyWALL.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.3 on page 40.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power adaptor to the ZyWALL.
5. If the problem continues, contact the vendor.

26.2 ZyWALL Access and Login

I forgot the IP address for the ZyWALL.

1. The default IP address is **192.168.167.1**.
2. If you changed the IP address and have forgotten it, you might get the IP address of the ZyWALL by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyWALL (it depends on the network), so enter this IP address in your Internet browser.
3. If this does not work, you have to reset the device to its factory defaults. See Section 26.6 on page 425.

I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 26.6 on page 425.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default LAN IP address is 192.168.167.1.
   - If you changed the IP address, use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for "I forgot the IP address for the ZyWALL." on page 420
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.3 on page 40.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix B on page 449.
4. Make sure your computer is in the same subnet as the ZyWALL. (If you know that there are routers between your computer and the ZyWALL, skip this step.)
5. Reset the device to its factory defaults, and try to access the ZyWALL with the default IP address. See Section 26.6 on page 425.
6. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the ZyWALL using another service, such as Telnet. If you can access the ZyWALL, use the commands to check the remote management settings, firewall rules, and filter settings to find out why the ZyWALL does not respond to HTTP.
- If your computer is connected to the **WAN** port, use a computer that is connected to a **LAN** port.
- You may also need to clear your Internet browser's cache. In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Option**s screen. In the **General** tab, click **Delete Files**. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it.
- If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address). In Windows, use **arp -d** at the command prompt to delete all entries in your computer's ARP table.

I can see the **Login** screen, but I cannot log in to the ZyWALL.

1. Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.
2. You cannot log in to the web configurator while someone already has a management session with the ZyWALL. Log out of the ZyWALL in the other session, or ask the person who is logged in to log out.
3. Disconnect and re-connect the power adaptor or cord to the ZyWALL.
4. If this does not work, you have to reset the device to its factory defaults. See Section 26.6 on page 425.

I cannot Telnet to the ZyWALL.

See the troubleshooting suggestions for "I cannot see or access the Login screen in the web configurator." on page 420. Ignore the suggestions about your browser.

Also see Section 18.1.1 on page 298 for conditions that block remote management sessions.

I cannot use FTP to upload new firmware or upload or download the configuration file.

See the troubleshooting suggestions for "I cannot see or access the Login screen in the web configurator." on page 420. Ignore the suggestions about your browser.

Also see Section 18.1.1 on page 298 for conditions that block remote management sessions.

Make sure you are uploading the correct configuration file or firmware for your specific model.

I cannot use SNMP to access or manage the ZyWALL.

See the troubleshooting suggestions for "I cannot see or access the Login screen in the web configurator." on page 420. Ignore the suggestions about your browser.

Also see Section 18.1.1 on page 298 for conditions that block remote management sessions.

I cannot use CNM Access to access or manage the ZyWALL.

See the troubleshooting suggestions for "I cannot see or access the Login screen in the web configurator." on page 420. Ignore the suggestions about your browser.

Also see Section 18.1.1 on page 298 for conditions that block remote management sessions.

Problems logging in to use a VPN tunnel.

Make sure you have entered the user name and password correctly. The fields are case-sensitive, so make sure [Caps Lock] is not on.

26.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.3 on page 40.
2. Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
4. If the problem continues, contact your ISP.

The ZyWALL is in bridge mode and my computer cannot get a dynamic IP address from a DHCP server on the WAN.

Enable the default WAN to LAN firewall rule for the **BOOTP_CLIENT** service.

I cannot access the Internet anymore. I had access to the Internet (through the ZyWALL), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.3 on page 40.
2. If you have a dynamically assigned WAN IP address, click the **Renew** button in the **HOME** screen.
3. Click **MAINTENANCE** > **Restart** > **Restart** to reboot the ZyWALL.
4. Disconnect and re-connect the power adaptor to the ZyWALL.
5. If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 26.1 on page 419. If the ZyWALL is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Click **MAINTENANCE** > **Restart** > **Restart** to reboot the ZyWALL.
3. Disconnect and re-connect the ZyWALL's power.
4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

I cannot play my online game.

Some game servers do not allow more than one login from the same IP address. If two users (behind the ZyWALL) want to connect to one of these servers at the same time, you need to use two different public IP addresses. Configure a many-to-many NAT rule to map the public IP addresses to the LAN IP addresses of the users that want to use the game server. See Chapter 16 on page 277 for details about NAT.

26.4 VoIP

I cannot make VoIP calls.

Click **ADVANCED > ALG** and enable either SIP or H.323 (whichever one you are using).

See Chapter 21 on page 331 for details on using SIP or H.323 through the ZyWALL.

I cannot receive VoIP calls.

See the troubleshooting suggestions for "I cannot make VoIP calls." on page 424.

You may also need to adjust the SIP timeout. Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the ZyWALL. If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout (default 60 minutes), the ZyWALL SIP ALG drops any incoming calls after the timeout period. Enter the SIP signaling session timeout value.

My VoIP calls are not clear.

There might be a lot of traffic on the network. Look at the LEDs, and check Section 26.1 on page 419. If the ZyWALL is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

26.5 Advanced Features

I cannot set up a VPN tunnel to another device.

If the IPSec tunnel does not build properly, the problem is likely a configuration error at one of the IPSec routers. Log into the web configurators of both IPSec routers (with the screens next to each other if possible). Check the VPN settings methodically and slowly.

The system log can also help identify a configuration problem. Click **LOGS** to see the system log. See Section 23.3.1 on page 357 for information on the log messages. You may need to click **LOGS > Log Settings** and make sure IKE and IPSec logging is enabled at both ends. Then clear the log and re-attempt to build the tunnel.

- The network policy must use **Tunnel** if there is a NAT router between the IPSec routers.

- If the sites are/were previously connected using a leased line or ISDN router, physically disconnect these devices from the network before testing your new VPN connection. The old route may have been learnt by RIP and would take priority over the new VPN connection.
- To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other.
  Before doing so, ensure that both computers have Internet access (through the IPSec routers).
- You can use the "**E-MAIL**" **Peer Type** and the "**SUBNET**" **Local** and **Remote Address Type** to simplify the configuration.
- Do not manually create any static IP routes for the remote VPN site. They are not required.

26.6 Resetting the ZyWALL to Its Factory Defaults

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button on the back of the ZyWALL. If you reset the ZyWALL, you lose all of the changes you have made. The ZyWALL re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

Make sure the **PWR** LED is on (not blinking) before you begin this procedure.

1. Press the **RESET** button in for about 10 seconds and release it. When the **PWR** LED starts to blink, the defaults have been restored and the ZyWALL restarts. If this does not restore the defaults, go to step 2.
2. Disconnect the ZyWALL's power.
3. While pressing the **RESET** button, reconnect the ZyWALL's power.
4. Continue to hold the **RESET** button. The **PWR** LED will begin to blink. This indicates that the defaults have been restored. Release the **RESET** button.
5. Wait for the ZyWALL to finish restarting before accessing again.

26.7 Packet Flow

The following is the packet check flow on the ZyWALL.

LAN to WAN: LAN Data and Call Filtering -> Firewall -> IDP -> Anti-Virus -> Remote Node Data Filtering -> NAT

WAN to LAN: Remote Node Data Filtering -> NAT -> Firewall -> IDP -> Anti-Virus -> LAN Data Filtering

27

Product Specifications

See also the Introduction chapter for a general overview of the key features.

27.1 Specification Tables

Table 163 Hardware Specifications

Dimensions	129 mm (L) x 82 mm (W) x 20 mm (H)
Weight	130 g
Ethernet Interface	
LAN	One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
WAN	One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
Reset Button	Restores factory default settings
Operation Temperature	0º C ~ 50º C
Storage Temperature	-30º C ~ 60º C
Operation Humidity	20% ~ 95% RH (non-condensing)
Storage Humidity	20% ~ 95% RH (non-condensing)
Certifications	EMC: FCC Class B, CE-EMC Class B, C-Tick Class B, VCCI Class B Safety: CSA International, CE EN60950-1

Only upload firmware for your specific model!

Table 164 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	192.168.167.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Default DHCP Pool Starting Address	192.168.167.33
Maximum DHCP Pool Size	32

Table 164 Firmware Specifications

FEATURE	DESCRIPTION
Device Management	Use the web configurator to easily configure the rich range of features on the ZyWALL.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyWALL.
Configuration Backup & Restoration	Make a copy of the ZyWALL's configuration. You can put it back on the ZyWALL later if you decide to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyWALL assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyWALL supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
IP Alias	IP alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the ZyWALL itself as the gateway for each subnet.
Bridge Mode	The ZyWALL can function as a transparent firewall. The ZyWALL bridges traffic traveling between the ZyWALL's interfaces and still filters and inspects packets. You do not need to change the configuration of your existing network.
STP (Spanning Tree Protocol) / RSTP (Rapid STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.
Zero Configuration Mode	Zero configuration mode provides Internet and VPN access for mobile users or telecommuters with little or no configuration. The ZyWALL auto-detects and automatically configures many settings. It also provides extra protection against unauthorized access.
MAC Filter	You can specify which computers can access the ZyWALL based on their MAC addresses.
Time and Date	Get the current time and date from an external server when you turn on your ZyWALL. You can also set the time manually. These dates and times are then used in logs.
Logging and Tracing	Use packet tracing and logs for troubleshooting. You can send logs from the ZyWALL to an external syslog server.
PPPoE	PPPoE mimics a dial-up Internet access connection.
PPTP Encapsulation	Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The ZyWALL supports one PPTP connection at a time.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
RoadRunner Support	The ZyWALL supports Time Warner's RoadRunner Service in addition to standard cable modem services.

Table 164 Firmware Specifications

FEATURE	DESCRIPTION
Firewall	You can configure firewall on the ZyXEL Device for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.
Intrusion Detection and Prevention (IDP)	The ZyWALL can detect and take actions on malicious or suspicious packets and traffic flows.
Anti-Virus Scanner	The ZyWALL can scan files transmitting through the enabled interfaces into the network. The ZyWALL helps stop threats at the network edge before they reach the local host computers.
IPSec VPN Capability	A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. The ZyWALL VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.
X-Auth (Extended Authentication)	X-Auth provides added security for VPN by requiring each VPN client to use a username and password.
Certificates	The ZyWALL can use certificates (also called digital IDs) for authentication. Certificates are based on public-private key pairs.
Local User Database	The ZyWALL can store user accounts in an internal database and use it to authenticate VPN users.
RADIUS	The ZyWALL can work with a RADIUS (Remote Authentication Dial In User Service) server for user authentication, authorization and accounting.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyWALL.
SSH	You can use SSH (Secure SHell) to securely access the ZyWALL's command line interface for management.
HTTPS	HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL is a web protocol that encrypts and decrypts web sessions. Use HTTPS for secure web configurator access to the ZyWALL
SNMP	SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version one (SNMPv1).
Central Network Management	Central Network Management (CNM) allows an enterprise or service provider network administrator to manage your ZyWALL. The enterprise or service provider network administrator can configure your ZyWALL, perform firmware upgrades and do troubleshooting for you.

Table 165 Feature and Performance Specifications

FEATURE	SPECIFICATION
Number of Local User Database Entries	8
Number of DHCP Clients in Server Pool	32
Number of Static DHCP Table Entries	8
Number of Static Routes	12

Table 165 Feature and Performance Specifications

FEATURE	SPECIFICATION
Number of Port Forwarding Rules	12
Number of NAT Sessions	1500
Number of Address Mapping Rules	10
Simultaneous IPSec VPN Connections	1
Configurable IPSec VPN Network Policies (including network policies in the recycle bin)	5
Number of DDNS Entries	5
Number of User Licenses	Unlimited
Firewall Throughput (with NAT)	50 Mbps
VPN (AES) Throughput	30 Mbps

27.2 Cable Pin Assignments

Table 166 Ethernet Cable Pin Assignments

WAN / LAN ETHERNET CABLE PIN LAYOUT							
Straight-through				**Crossover**			
(Switch)			(Adapter)	(Switch)			(Switch)
1	IRD +		1 OTD +	1	IRD +		1 IRD +
2	IRD -		2 OTD -	2	IRD -		2 IRD -
3	OTD +		3 IRD +	3	OTD +		3 OTD +
6	OTD -		6 IRD -	6	OTD -		6 OTD -

27.3 Power Specifications

The ZyWALL gets power through a USB connection or an (optional) power adapter with the following specifications.

Table 167 AC Power Adaptor Specifications

AC Power Adapter model MU12-2050150-C5
Input power: 100 to 240 Volts AC (VAC), 60/50 Hz, maximum 0.5 A at 100 VAC
Output power: 5 Volts DC, maximum 1.5 A
Power consumption: 7.5 W
Plug: North American standards
Safety standards: UL, CE

PART VIII Appendices and Index

Setting up Your Computer's IP Address (433)
Pop-up Windows, JavaScripts and Java Permissions (449)
IP Addresses and Subnetting (455)
Common Services (463)
Windows 98 SE/Me Requirements for Anti-Virus Message Display (467)
Importing Certificates (471)
Command Interpreter (481)
NetBIOS Filter Commands (487)
Legal Information (489)
Customer Support (493)
Index (499)

A

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

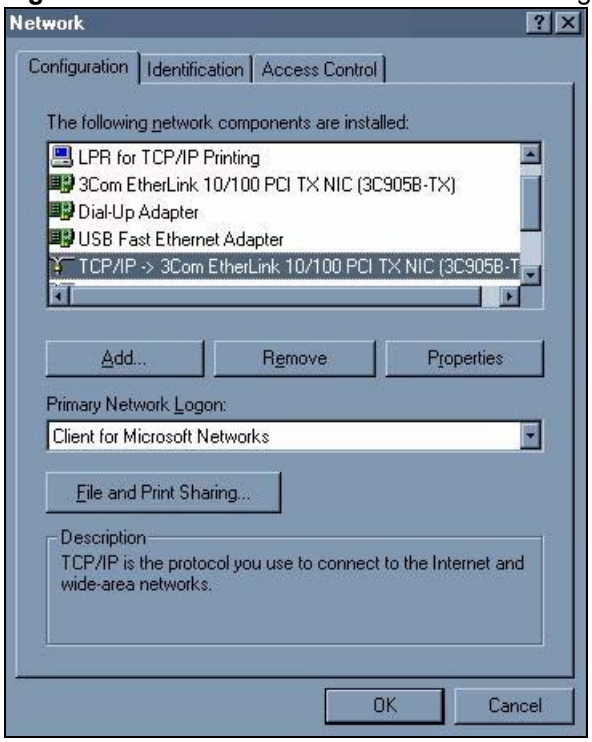
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyWALL's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 259 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.
3. Select **Microsoft** from the list of manufacturers.
4. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5. Restart your computer so the changes you made take effect.

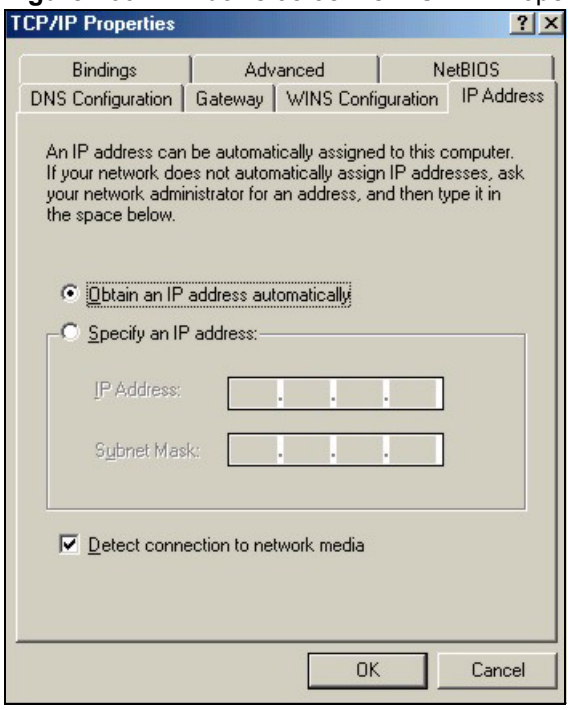
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

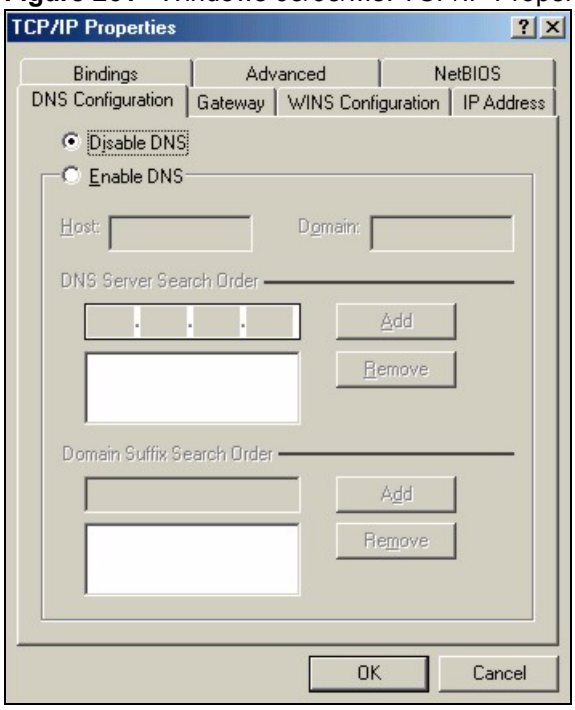
Figure 260 Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 261 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.
   - If you do not know your gateway's IP address, remove previously installed gateways.
   - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
5 Click **OK** to save and close the **TCP/IP Properties** window.
6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7 Turn on your ZyWALL and restart your computer when prompted.

Verifying Settings

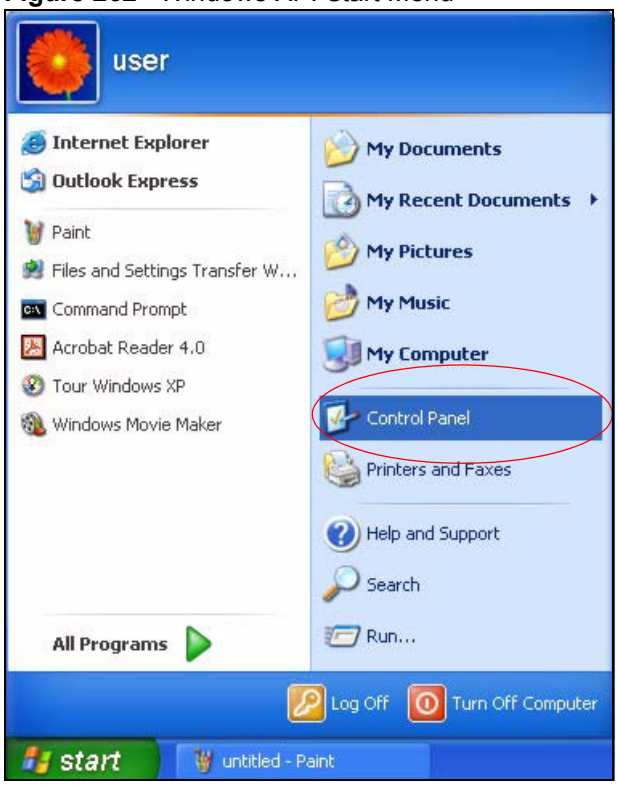
1 Click **Start** and then **Run**.
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 262 Windows XP: Start Menu

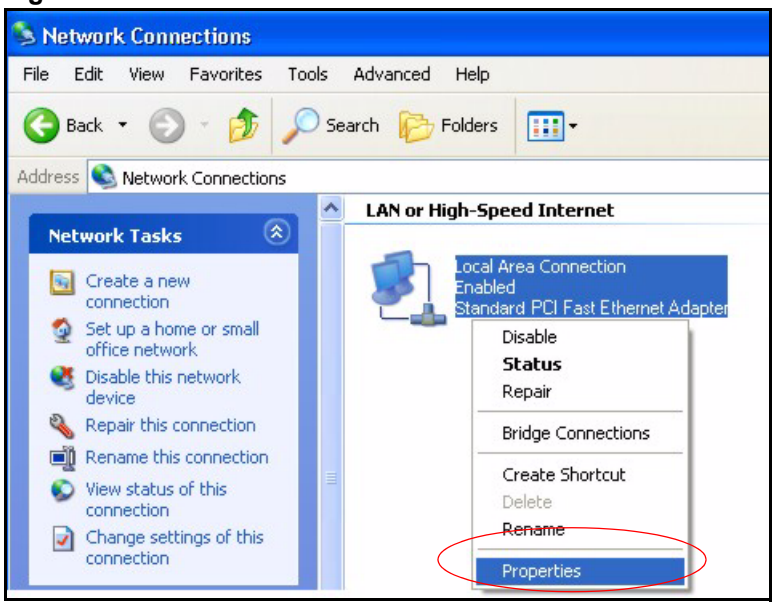


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 263 Windows XP: Control Panel

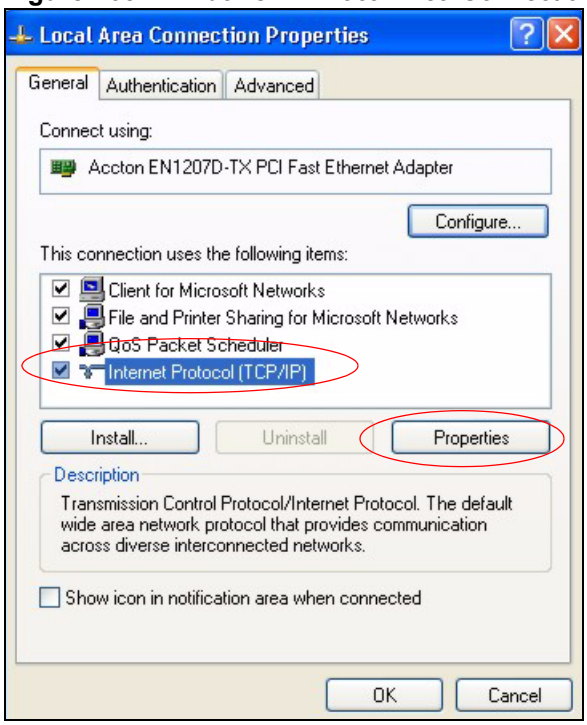
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 264 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

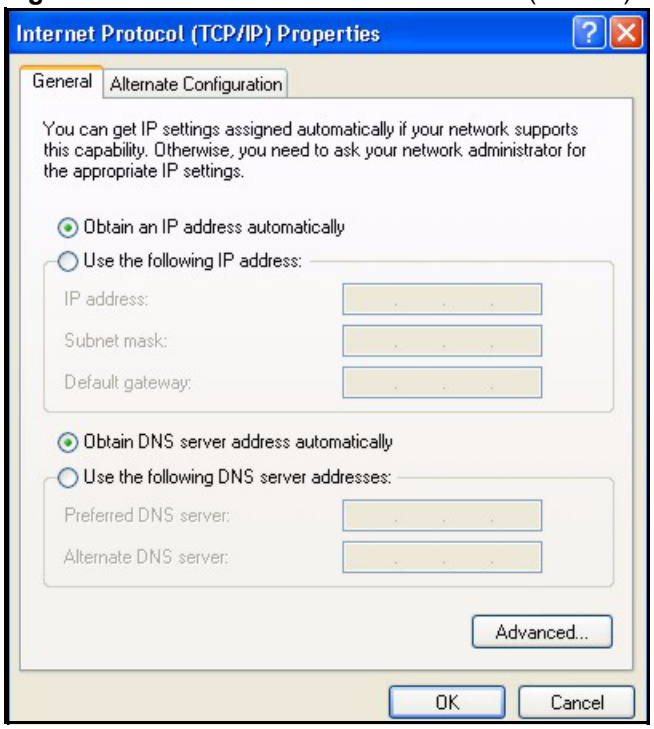
Figure 265 Windows XP: Local Area Connection Properties


Local Area Connection Properties
General Authentication Advanced
Connect using:
Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 266 Windows XP: Internet Protocol (TCP/IP) Properties

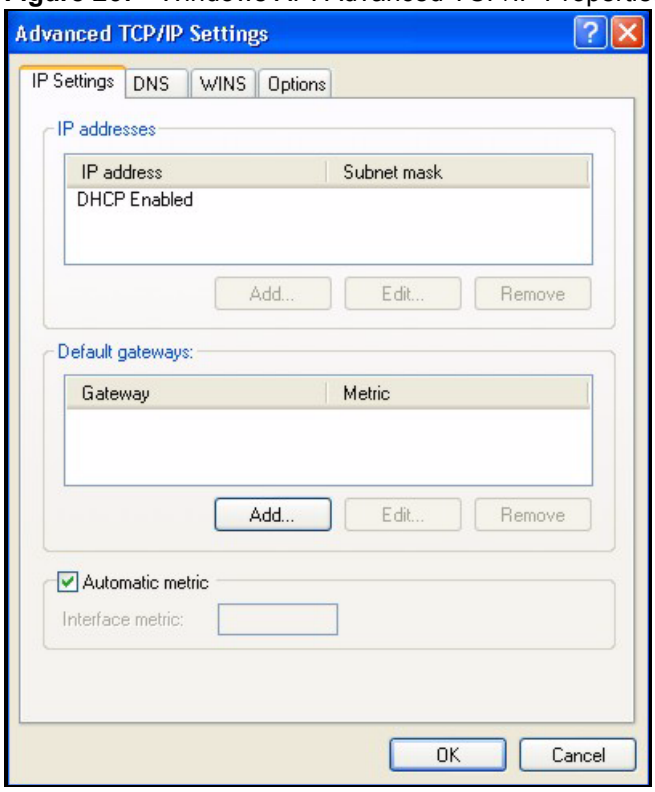

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 267 Windows XP: Advanced TCP/IP Properties

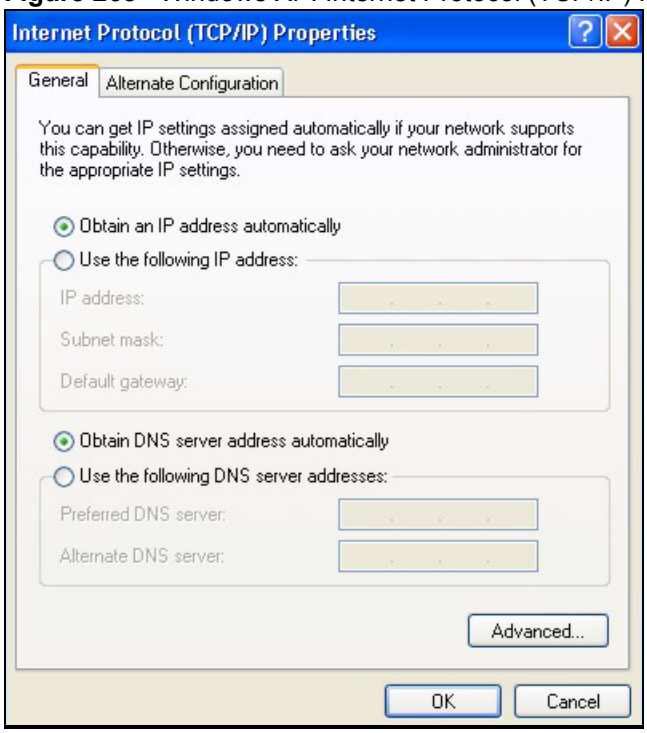


7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 268 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your ZyWALL and restart your computer (if prompted).

Verifying Settings

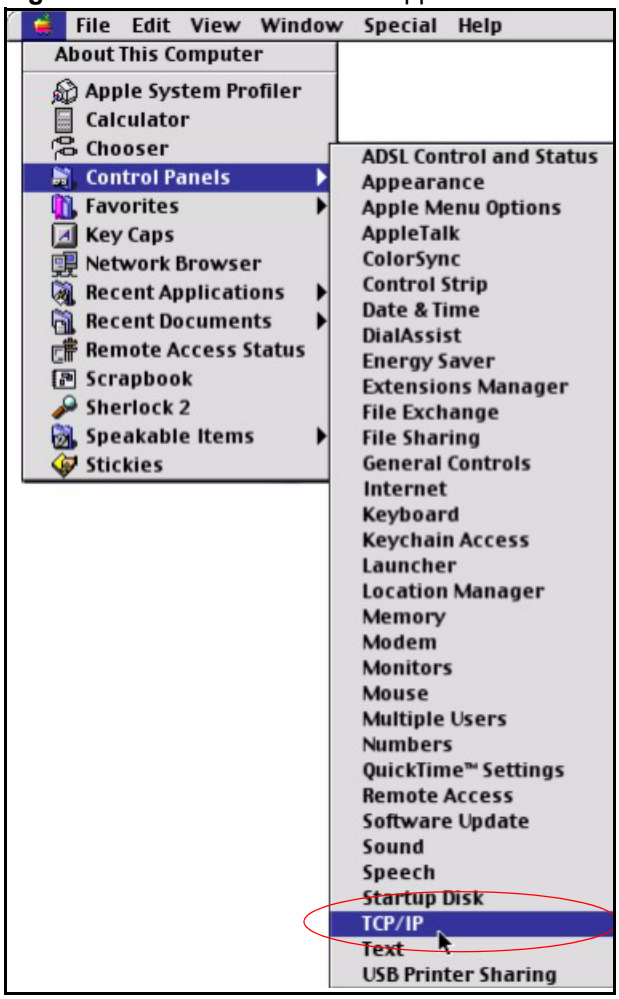
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

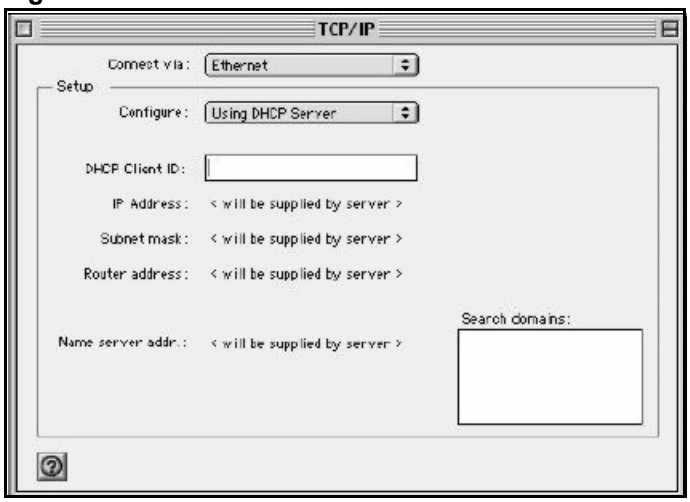
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 269 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 270 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyWALL in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your ZyWALL and restart your computer (if prompted).

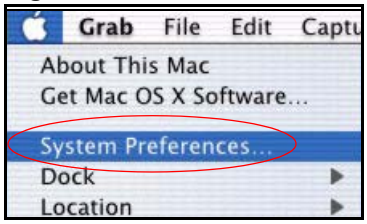
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 271 Macintosh OS X: Apple Menu

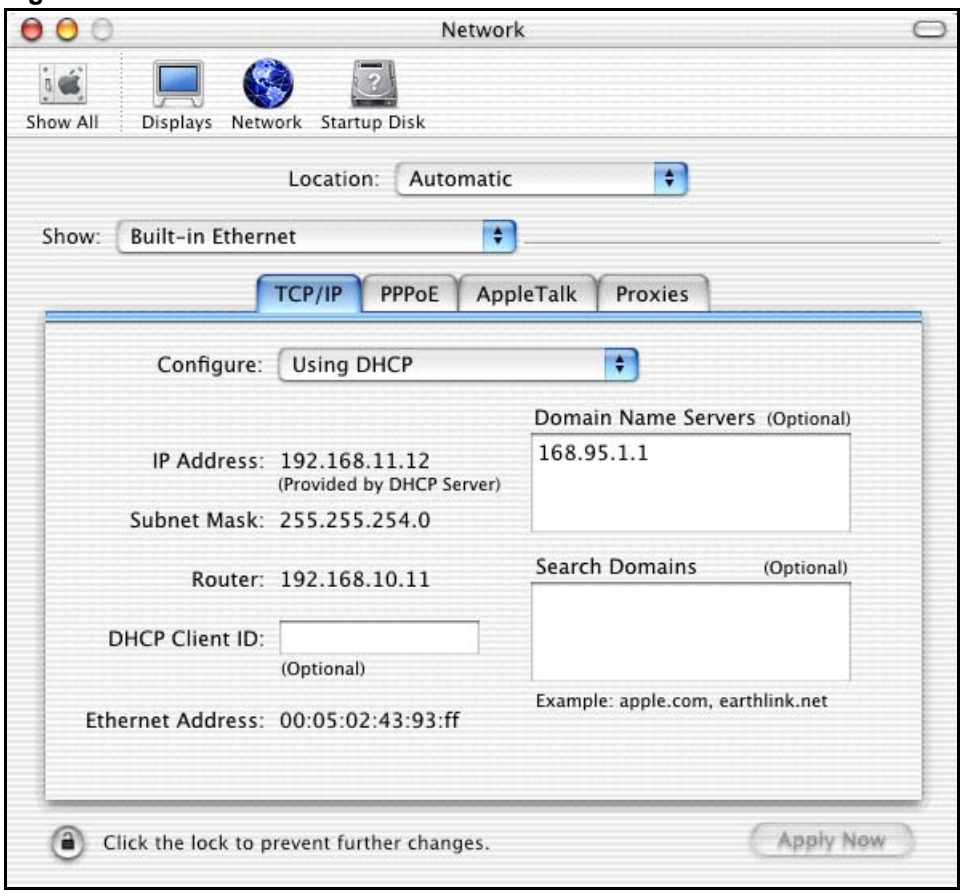


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 272 Macintosh OS X: Network



4 For statically assigned settings, do the following:
   - From the **Configure** box, select **Manually**.
   - Type your IP address in the **IP Address** box.
   - Type your subnet mask in the **Subnet mask** box.
   - Type the IP address of your ZyWALL in the **Router address** box.
5 Click **Apply Now** and close the window.
6 Turn on your ZyWALL and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

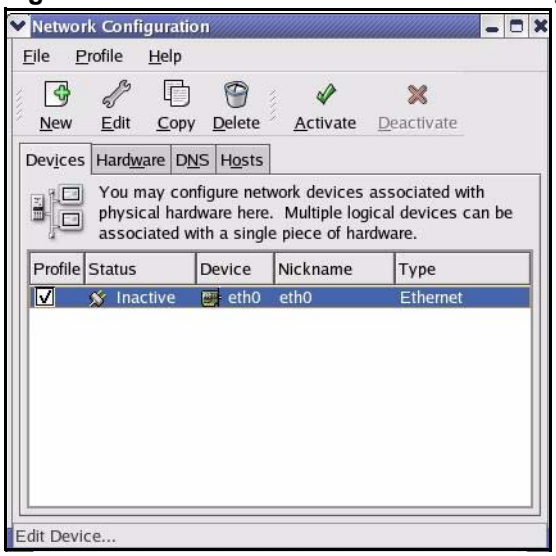
Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 273 Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

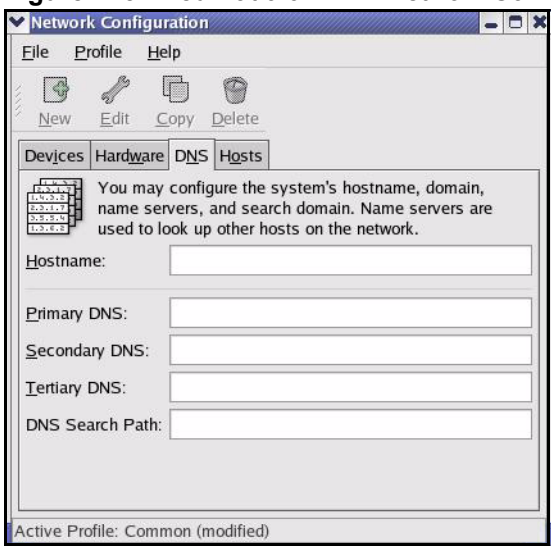
Figure 274 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 275 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 276 Red Hat 9.0: KDE: Network Configuration: Activate

Question
redhat-config-network:
You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.
Do you want to continue?
No
Yes

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 277 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the BOOTPROTO= field. Type IPADDR= followed by the IP address (in dotted decimal notation) and type NETMASK= followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 278 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2. If you know your DNS server IP address(es), enter the DNS server information in the resolv.conf file in the /etc directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 279 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3. After you edit and save the configuration files, you must restart the network card. Enter ./network restart in the /etc/rc.d/init.d directory. The following figure shows an example.

Figure 280 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 281 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

B

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

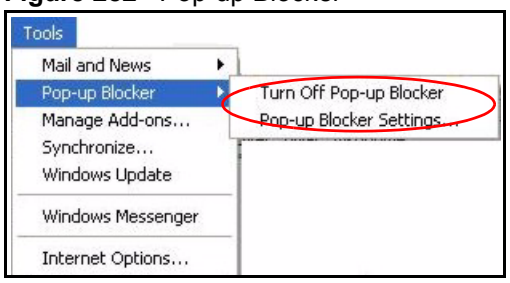
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 282 Pop-up Blocker

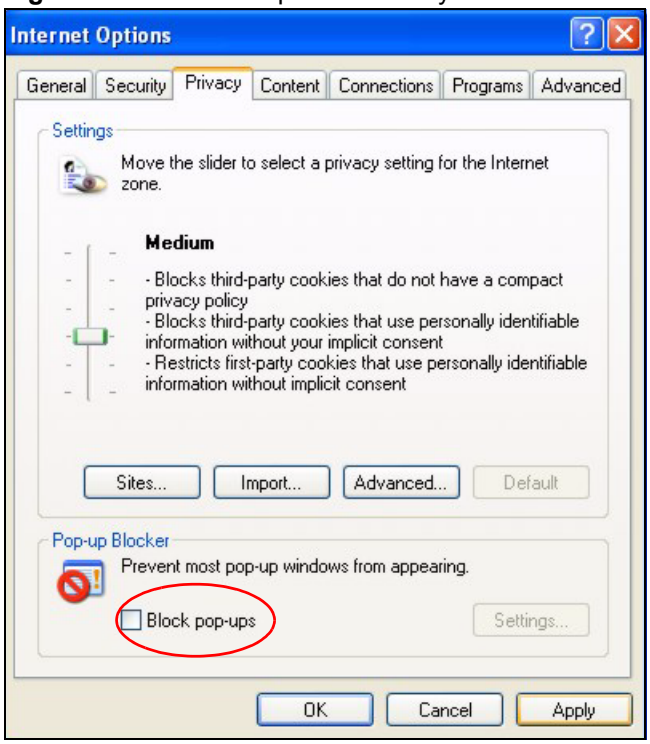


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 283 Internet Options: Privacy



3 Click **Apply** to save this setting.

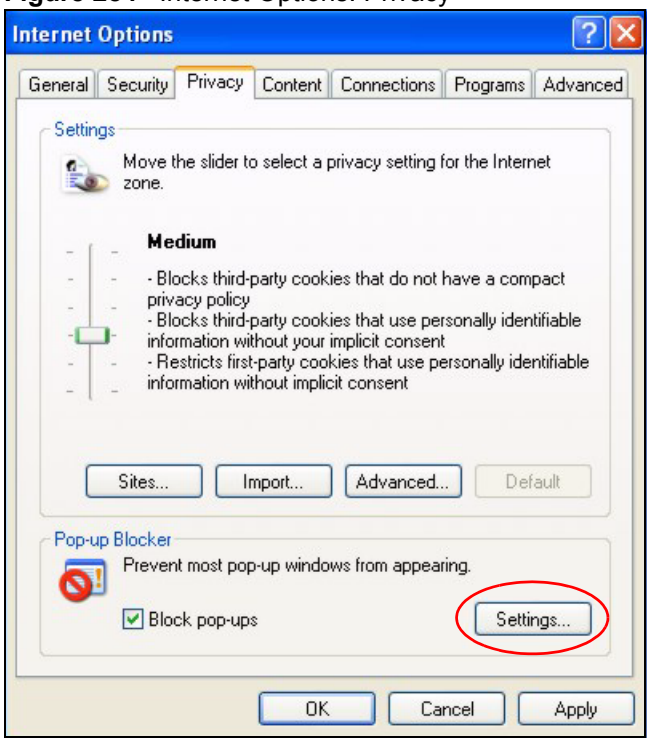
Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

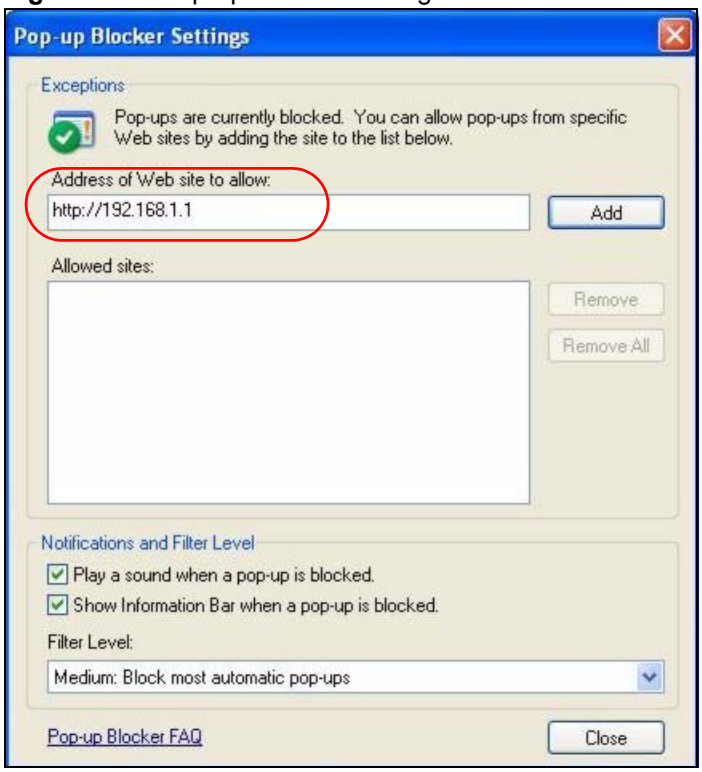
Figure 284 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 285 Pop-up Blocker Settings


Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

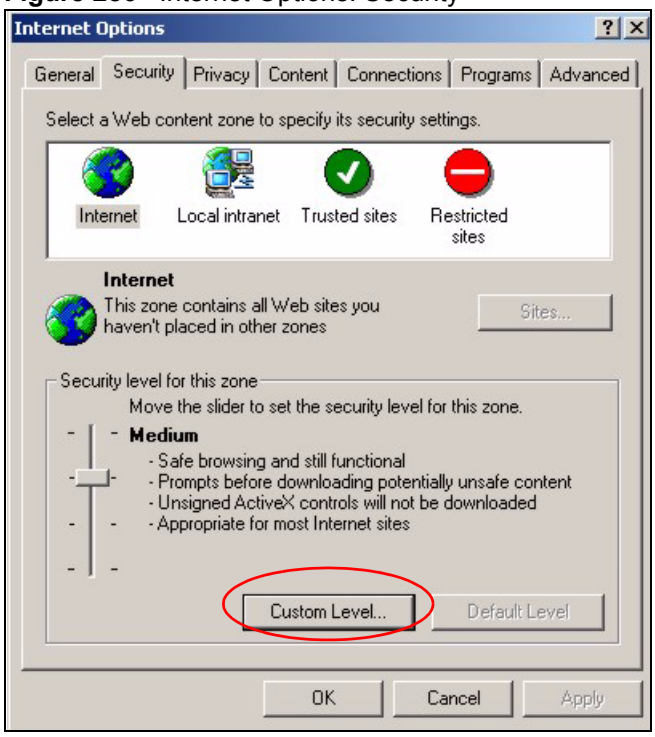
5 Click **Close** to return to the **Privacy** screen.
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

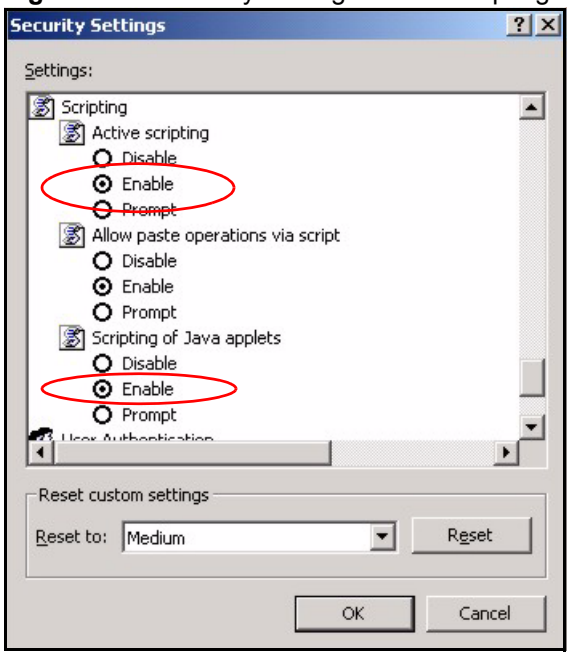
1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 286 Internet Options: Security



2 Click the **Custom Level...** button.
3 Scroll down to **Scripting**.
4 Under **Active scripting** make sure that **Enable** is selected (the default).
5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
6 Click **OK** to close the window.

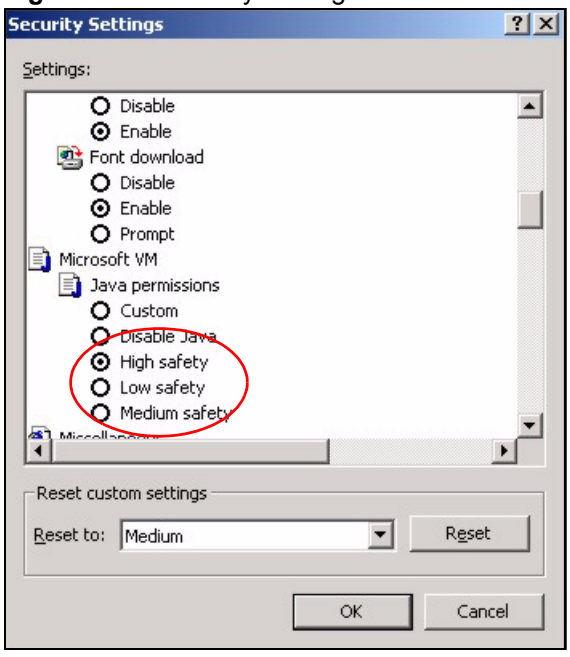
Figure 287 Security Settings - Java Scripting



Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

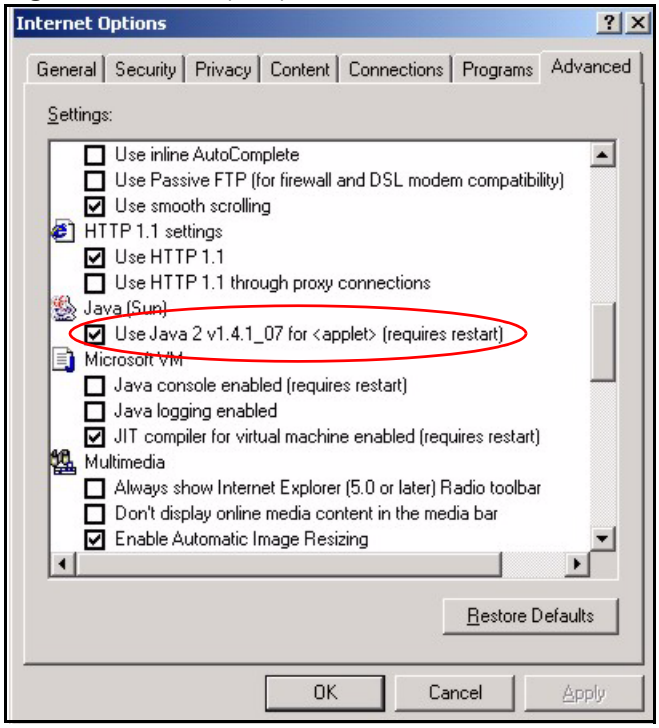
Figure 288 Security Settings - Java



JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3 Click **OK** to close the window.

Figure 289 Java (Sun)



C

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

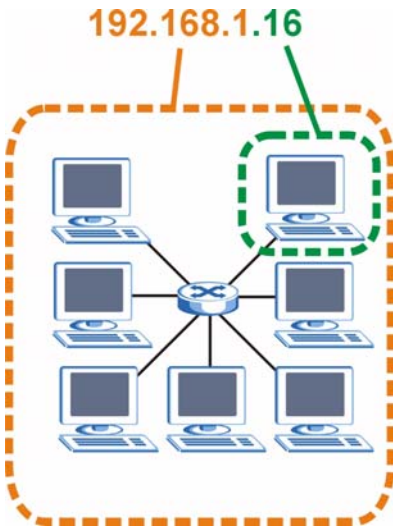
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 290 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 168 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 169 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 170 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 171 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 171 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

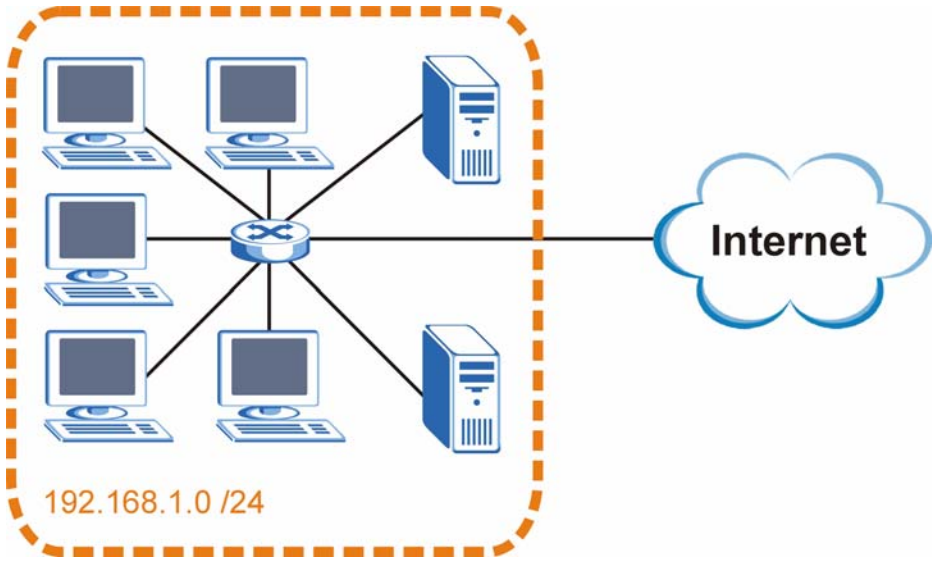
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 291 Subnetting Example: Before Subnetting

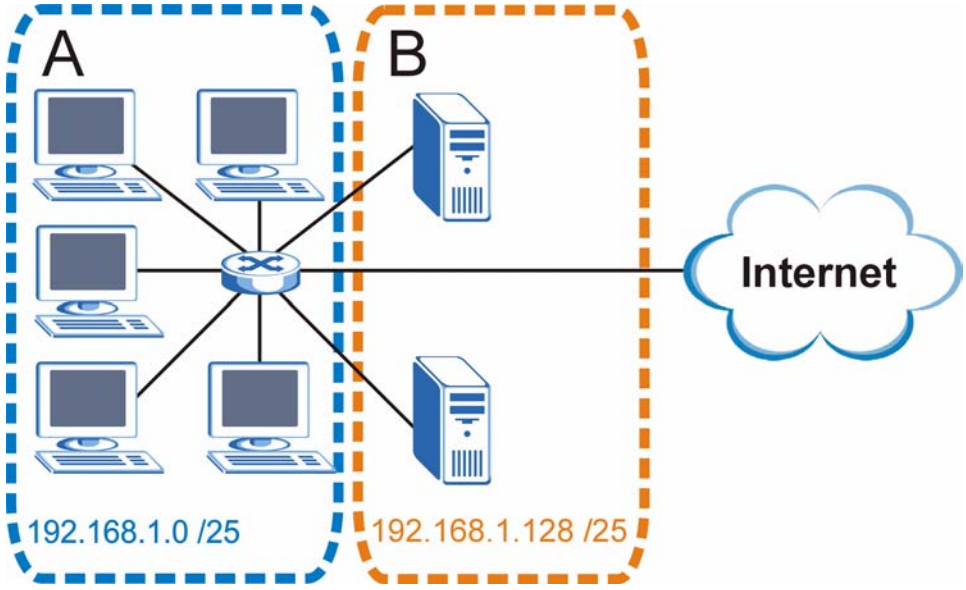


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 292 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 172 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 173 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 174 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 175 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 176 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 176 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 177 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 178 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 178 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyWALL.

Once you have decided on the network number, pick an IP address for your ZyWALL that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyWALL will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyWALL unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

D

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 179 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.

Table 179 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.

Table 179 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

E

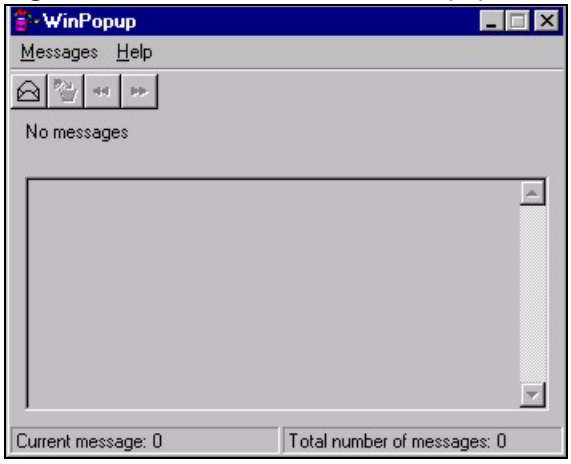
Windows 98 SE/Me Requirements for Anti-Virus Message Display

With the anti-virus packet scan, when a virus is detected, an alert message is displayed on Miscrosoft Windows-based computers.

For Windows 98 SE/Me, you must open the **WinPopup** window in order to view real-time alert messages. For Windows 2000 and later versions, a message window automatically displays when an alert is received.

Click **Start**, **Run** and enter “winpopup” in the field provided and click **OK**. The **WinPopup** window displays as shown.

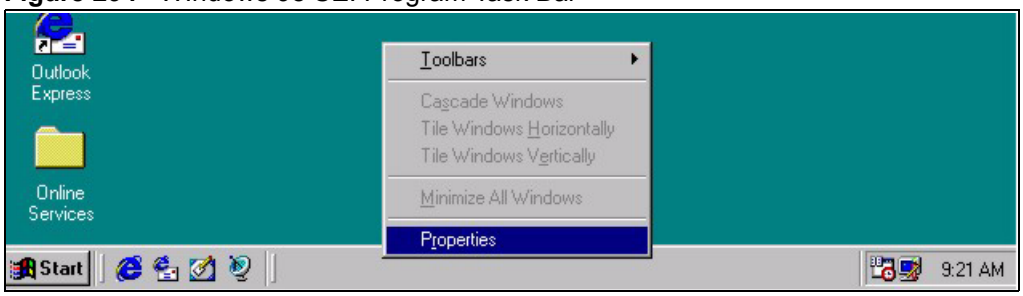
Figure 293 Windows 98 SE: WinPopup



If you want to display the WinPopup window at startup, follow the steps below for Windows 98 SE (steps are similar for Windows Me).

1 Right-click on the program task bar and click **Properties**.

Figure 294 WIndows 98 SE: Program Task Bar



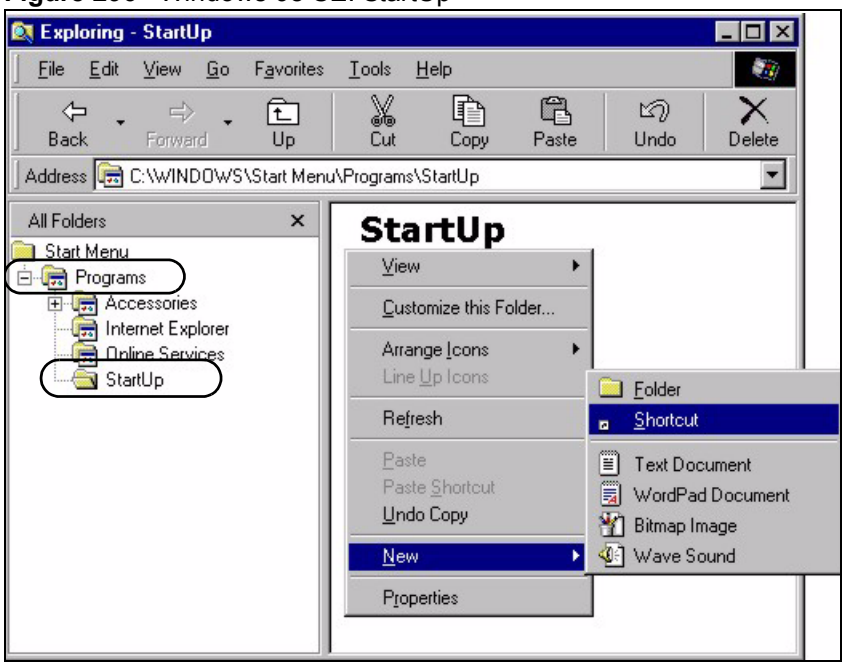
2 Click the **Start Menu Programs** tab and click **Advanced ..**.

Figure 295 Windows 98 SE: Task Bar Properties

3 Double-click **Programs** and click **StartUp**.

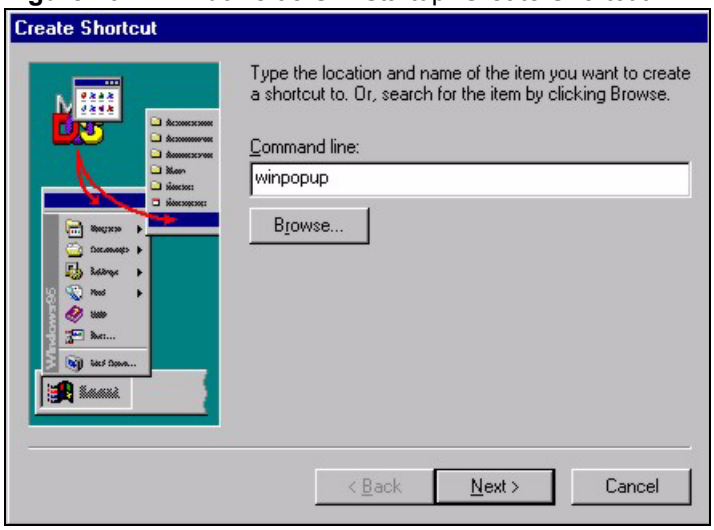
4 Right-click in the **StartUp** pane and click **New**, **Shortcut**.

Figure 296 Windows 98 SE: StartUp



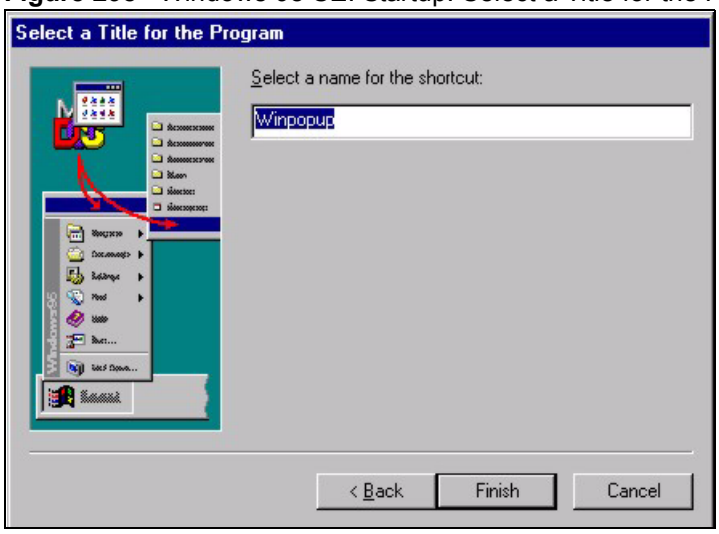
5 A **Create Shortcut** window displays. Enter "winpopup" in the **Command line** field and click **Next**.

Figure 297 Windows 98 SE: Startup: Create Shortcut


Create Shortcut
Type the location and name of the item you want to create a shortcut to. Or, search for the item by clicking Browse.
Command line:
winpopup
Browse...
< Back
Next >
Cancel

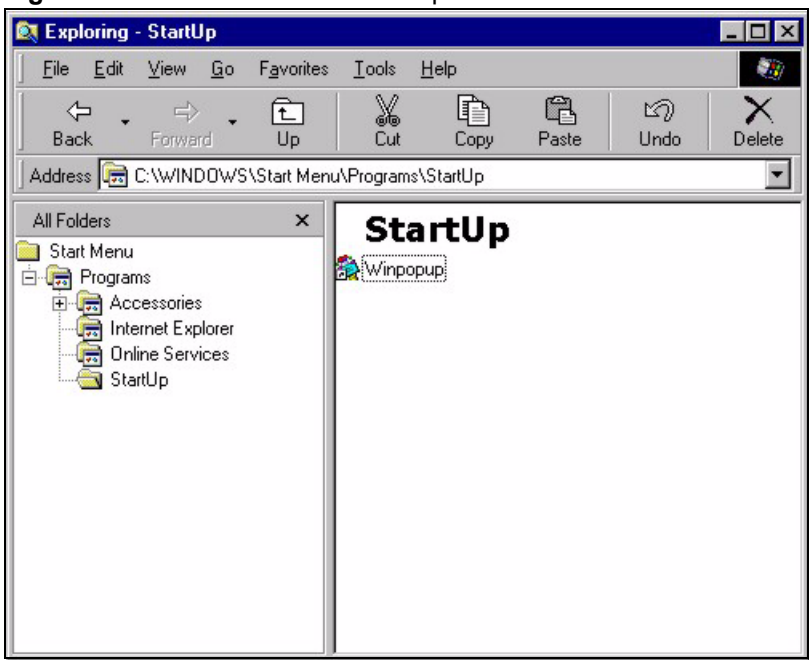
6 Specify a name for the shortcut or accept the default and click **Finish**.

Figure 298 Windows 98 SE: Startup: Select a Title for the Program



7 A shortcut is created in the **StartUp** pane. Restart the computer when prompted.

Figure 299 Windows 98 SE: Startup: Shortcut



The WinPopup window displays after the computer finishes the startup process (see Figure 293 on page 467).

F

Importing Certificates

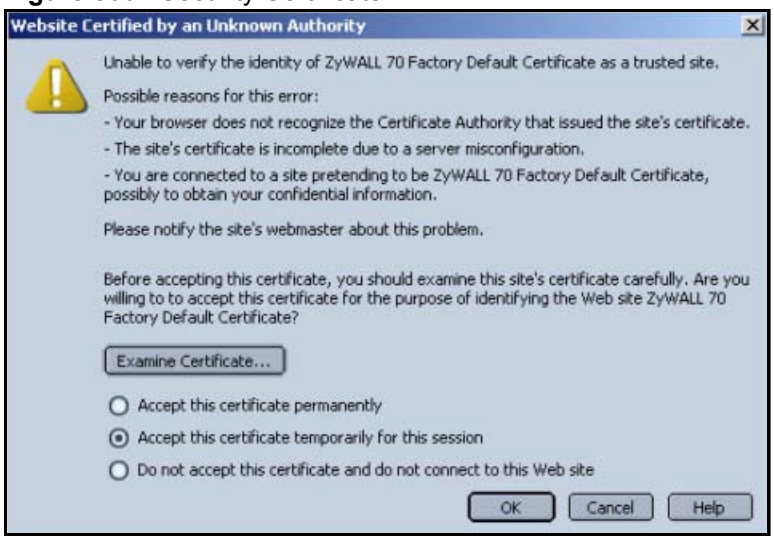
This appendix shows importing certificates examples using Internet Explorer 5.

Import ZyWALL Certificates into Netscape Navigator

In Netscape Navigator, you can permanently trust the ZyWALL's server certificate by importing it into your operating system as a trusted certification authority.

Select **Accept This Certificate Permanently** in the following screen to do this.

Figure 300 Security Certificate


Website Certified by an Unknown Authority
Unable to verify the identity of ZyWALL 70 Factory Default Certificate as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be ZyWALL 70 Factory Default Certificate, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site ZyWALL 70 Factory Default Certificate?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
OK
Cancel
Help

Importing the ZyWALL's Certificate into Internet Explorer

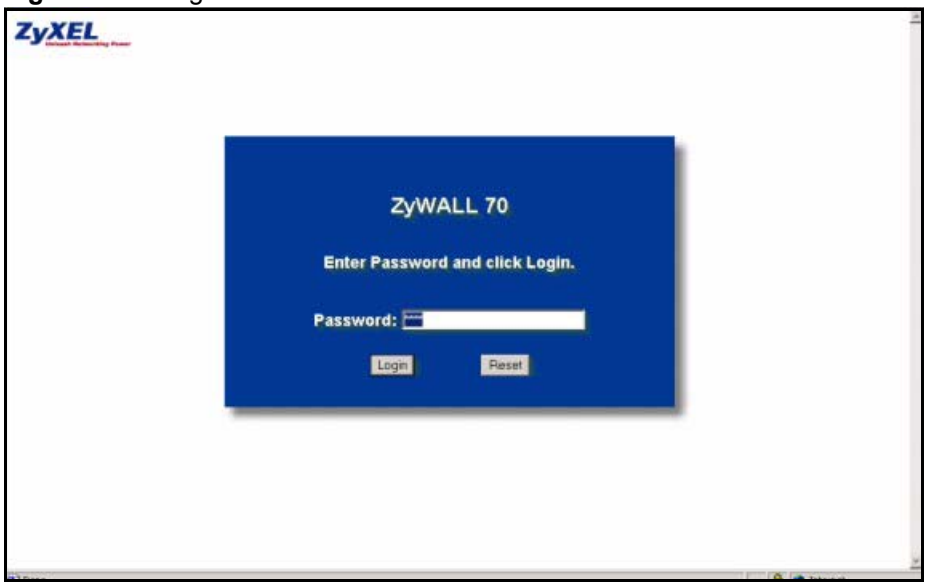
For Internet Explorer to trust a self-signed certificate from the ZyWALL, simply import the self-signed certificate into your operating system as a trusted certification authority.

To have Internet Explorer trust a ZyWALL certificate issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certification authority.

The following example procedure shows how to import the ZyWALL's (self-signed) server certificate into your operating system as a trusted certification authority.

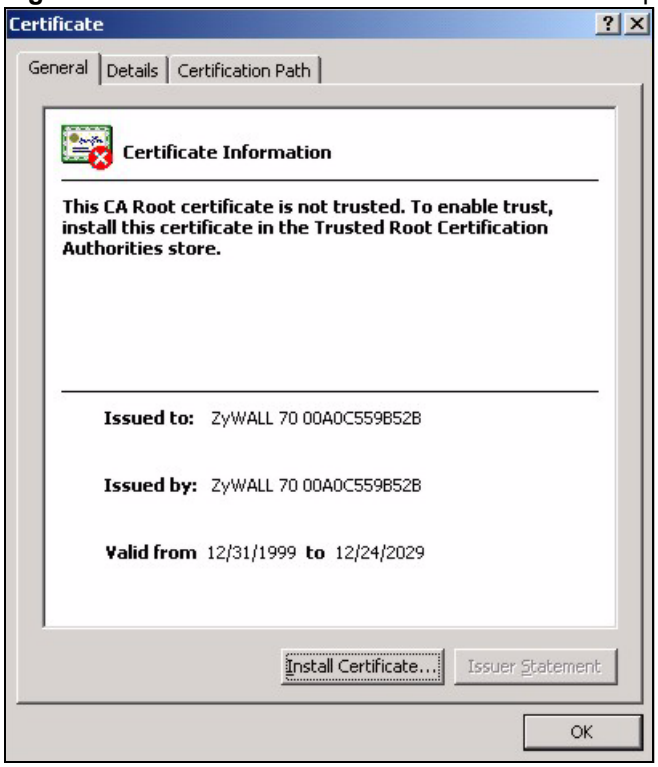
1 In Internet Explorer, double click the lock shown in the following screen.

Figure 301 Login Screen



2 Click **Install Certificate** to open the **Install Certificate** wizard.

Figure 302 Certificate General Information before Import



3 Click **Next** to begin the **Install Certificate** wizard.

Figure 303 Certificate Import Wizard 1

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

4 Select where you would like to store the certificate and then click **Next**.

Figure 304 Certificate Import Wizard 2

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

5 Click **Finish** to complete the **Import Certificate** wizard.

Figure 305 Certificate Import Wizard 3

6 Click **Yes** to add the ZyWALL certificate to the root store.

Figure 306 Root Certificate Store

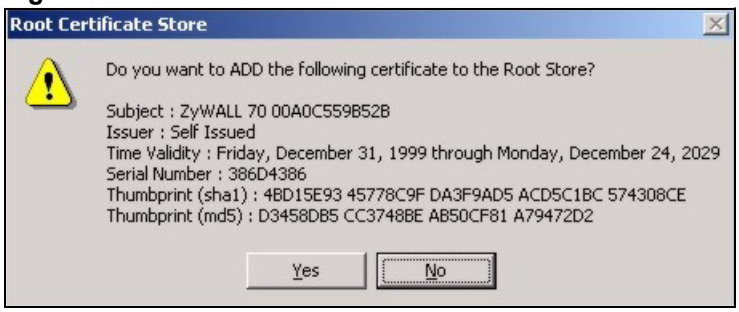
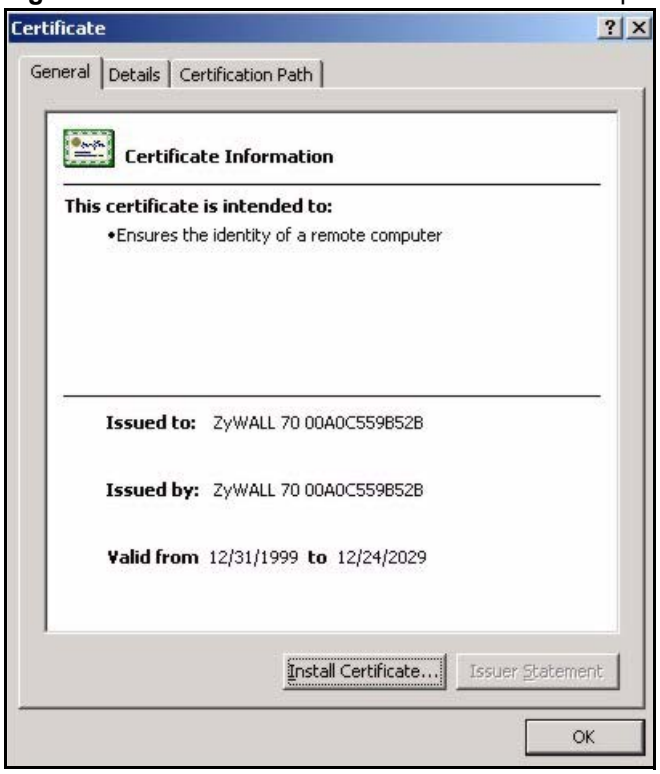

Root Certificate Store
Do you want to ADD the following certificate to the Root Store?
Subject : ZyWALL 70 00A0C559B52B
Issuer : Self Issued
Time Validity : Friday, December 31, 1999 through Monday, December 24, 2029
Serial Number : 386D4386
Thumbprint (sha1) : 4BD15E93 45778C9F DA3F9AD5 ACD5C1BC 574308CE
Thumbprint (md5) : D3458DB5 CC3748BE AB50CF81 A79472D2
Yes
No

Figure 307 Certificate General Information after Import



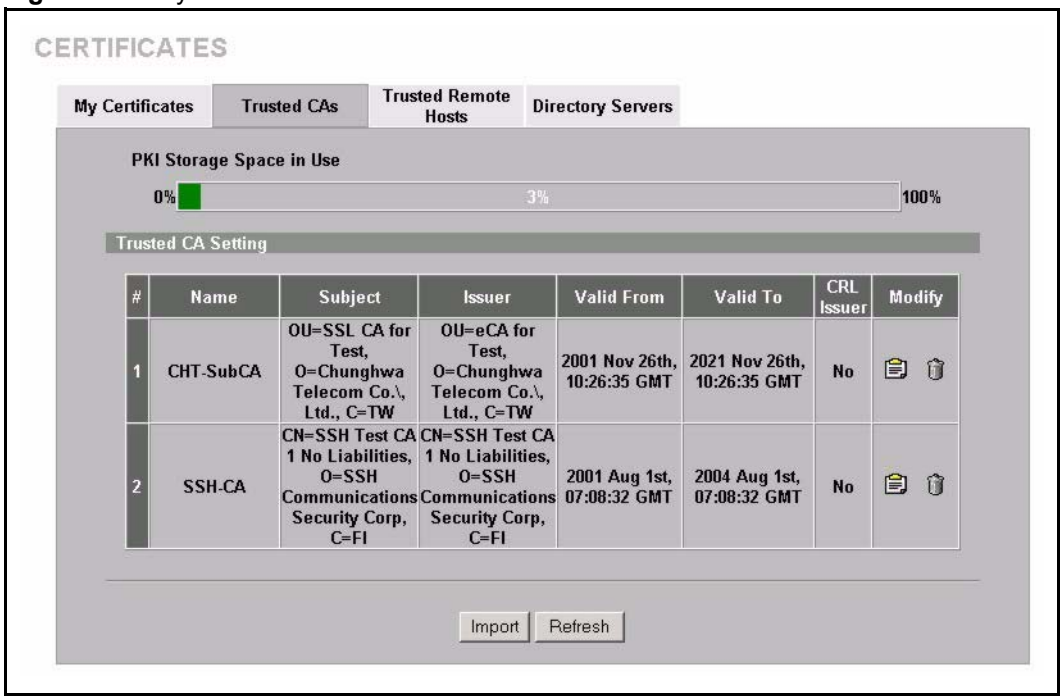
Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the ZyWALL.

You must have imported at least one trusted CA to the ZyWALL in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the ZyWALL (see the ZyWALL's **Trusted CA** web configurator screen).

Figure 308 ZyWALL Trusted CA Screen

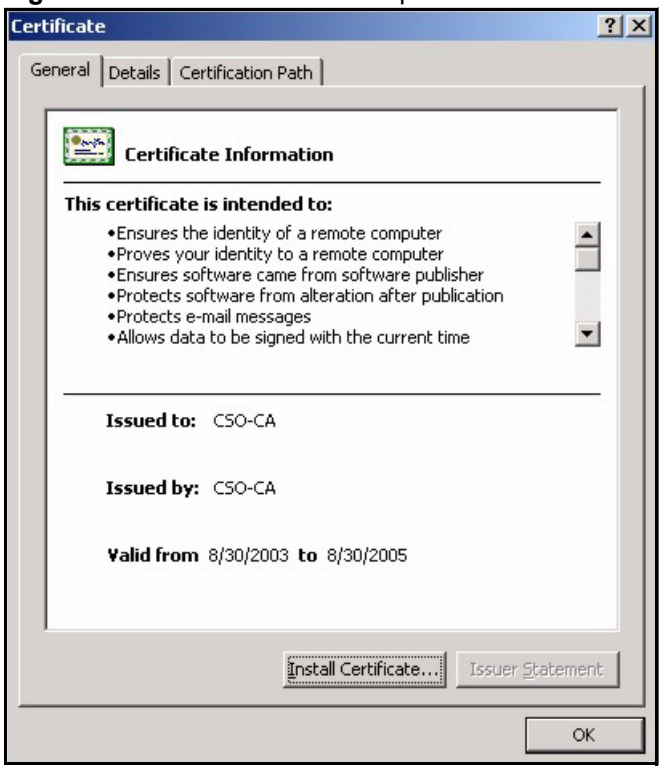

CERTIFICATES
My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers
PKI Storage Space in Use
0%
3%
100%
Trusted CA Setting
Name Subject Issuer Valid From Valid To CRL Issuer Modify
1 CHT-SubCA OU=SSL CA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW 2001 Nov 26th, 10:26:35 GMT 2021 Nov 26th, 10:26:35 GMT No
2 SSH-CA CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI 2001 Aug 1st, 07:08:32 GMT 2004 Aug 1st, 07:08:32 GMT No
Import
Refresh

The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

Installing the CA's Certificate

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

Figure 309 CA Certificate Example



2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

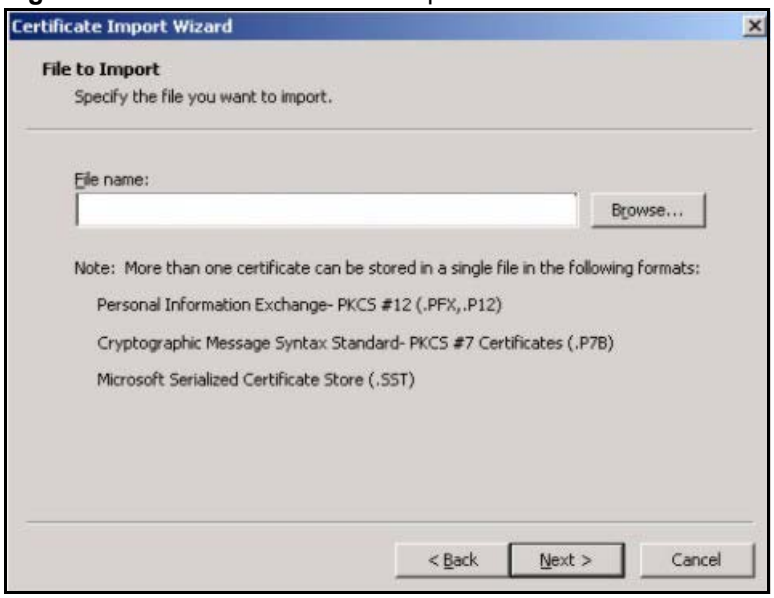
1 Click **Next** to begin the wizard.

Figure 310 Personal Certificate Import Wizard 1

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

Figure 311 Personal Certificate Import Wizard 2


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
< Back
Next >
Cancel

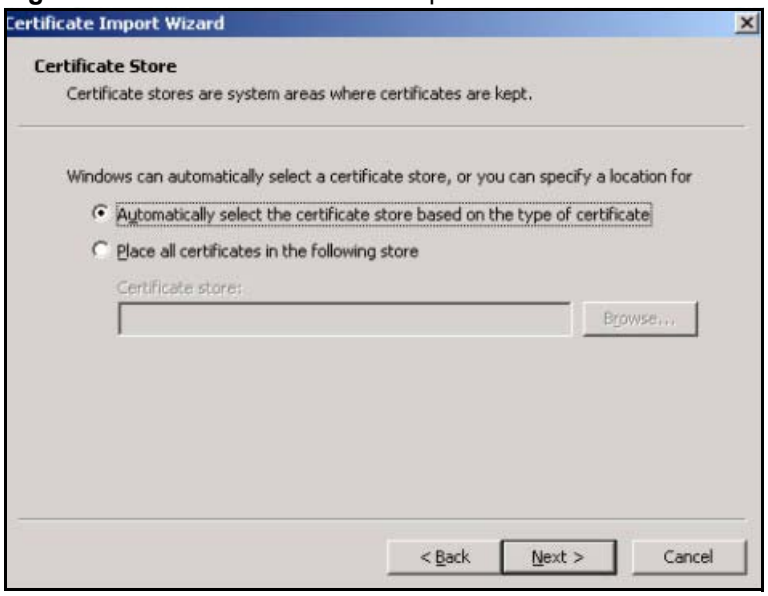
3 Enter the password given to you by the CA.

Figure 312 Personal Certificate Import Wizard 3

Certificate Import Wizard
Password
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark the private key as exportable
< Back
Next >
Cancel

4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

Figure 313 Personal Certificate Import Wizard 4


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

5 Click **Finish** to complete the wizard and begin the import process.

Figure 314 Personal Certificate Import Wizard 5

6 You should see the following screen when the certificate is correctly installed on your computer.

Figure 315 Personal Certificate Import Wizard 6

Using a Certificate When Accessing the ZyWALL Example

Use the following procedure to access the ZyWALL via HTTPS.

1 Enter 'https://ZyWALL IP Address/ in your browser's web address field.

Figure 316 Access the ZyWALL Via HTTPS

about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://192.168.1.1

2 When **Authenticate Client Certificates** is selected on the ZyWALL, the following screen asks you to select a personal certificate to send to the ZyWALL. This screen displays even if you only have a single certificate as in the example.

Figure 317 SSL Client Authentication

3 You next see the ZyWALL login screen.

Figure 318 ZyWALL Secure Login Screen

G

Command Interpreter

The following describes how to use the command interpreter. See Section 18.13 on page 311 for how to log into the command interpreter. See the included disk or zyxel.com for more detailed information on these commands.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets <>.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means or.
  For example,
  sys filter netbios config <type> <on|off>
  means that you must specify the type of netbios filter and whether to turn it on or off.

Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to close the session when finished.

Command Examples

This section provides some examples of commands you can use on the ZyWALL. This list is intended as a general reference of examples. The commands available in your ZyWALL may differ from the examples given here. See the other appendices for more examples.

Configuring What You Want the ZyWALL to Log

1. Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyWALL is to record.
2. Use `sys logs category` to view a list of the log categories.

Figure 319 Displaying Log Categories Example

```
ras> sys logs category
8021x           access          attack          display
error           icmp            ike             ipsec
javablocked     mten            packetfilter    ppp
cdr             pki             tls             remote
tcpreset        traffic         upnp            urlblocked
urlforward      wireless
```

3. Use `sys logs category` followed by a log category to display the parameters that are available for the category.

Figure 320 Displaying Log Parameters Example

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both] [0:don't show debug type/1:show debug
type]
```

4. Use `sys logs category` followed by a log category and a parameter to decide what to record.

   Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.
5. Use the `sys logs save` command to store the settings in the ZyWALL (you must do this in order to record logs).

Displaying Logs

- Use the `sys logs display` command to show all of the logs in the ZyWALL's log.
- Use the `sys logs category display` command to show the log settings for all of the log categories.
- Use the `sys logs display [log category]` command to show the logs in an individual ZyWALL log category.
- Use the `sys logs clear` command to erase all of the ZyWALL's logs.

Log Command Example

This example shows how to set the ZyWALL to record the access logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access

#  .time                 source                 destination            notes

    message
  0|06/08/2004 05:58:21 |172.21.4.154          |224.0.1.24            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  1|06/08/2004 05:58:20 |172.21.3.56           |239.255.255.250       |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  2|06/08/2004 05:58:20 |172.21.0.2            |239.255.255.254       |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  3|06/08/2004 05:58:20 |172.21.3.191          |224.0.1.22            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  4|06/08/2004 05:58:20 |172.21.0.254          |224.0.0.1             |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  5|06/08/2004 05:58:20 |172.21.4.187:137      |172.21.255.255:137    |ACCESS
BLOCK
    Firewall default policy: UDP (W to W/ZW)
```

Routing Command

Syntax: `ip nat routing [0:LAN] [0:no|1:yes]`

Use this command to set the ZyWALL to route traffic that does not match a NAT rule through a specific interface. An example of when you may want to use this is if you have servers with public IP addresses connected to the LAN.

The following command example sets the ZyWALL to route traffic that does not match a NAT rule through the LAN interface.

Figure 321 Routing Command Example

```
ras> ip nat routing 2 0
Routing can work in NAT when no NAT rule match.
-----------------------------------------------
         LAN: yes
```

ARP Behavior and the ARP ackGratuitous Commands

The ZyWALL does not accept ARP reply information if the ZyWALL did not send out a corresponding request. This helps prevent the ZyWALL from updating its ARP table with an incorrect IP address to MAC address mapping due to a spoofed ARP. An incorrect IP to MAC address mapping in the ZyWALL's ARP table could cause the ZyWALL to send packets to the wrong device.

Commands for Using or Ignoring Gratuitous ARP Requests

A host can send an ARP request to resolve its own IP address. This is called a gratuitous ARP request. The packet uses the host's own IP address as the source and destination IP address. The packet uses the Ethernet broadcast address (FF:FF:FF:FF:FF:FF) as the destination MAC address. This is used to determine if any other hosts on the network are using the same IP address as the sending host. The other hosts in the network can also update their ARP table IP address to MAC address mappings with this host's MAC address.

The `ip arp ackGratuitous` commands set how the ZyWALL handles gratuitous ARP requests.

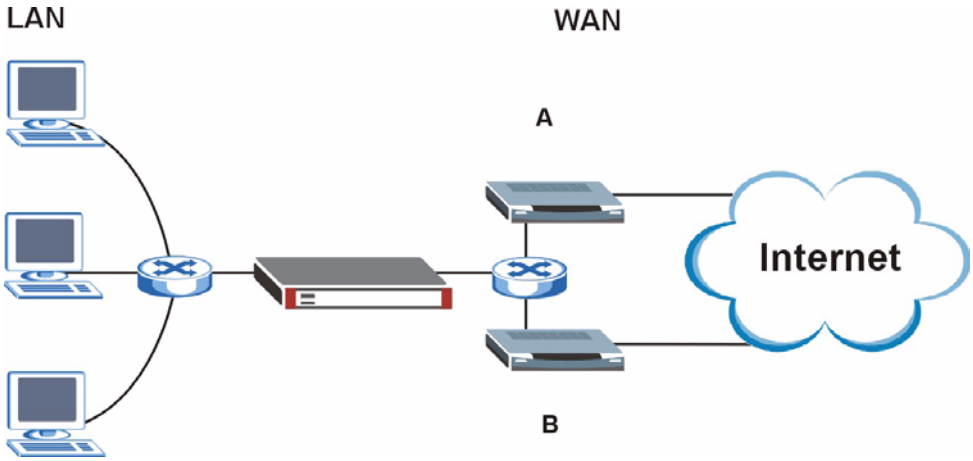
- Use `ip arp ackGratuitous active no` to have the ZyWALL ignore gratuitous ARP requests.
- Use `ip arp ackGratuitous active yes` to have the ZyWALL respond to gratuitous ARP requests.

  For example, say the regular gateway goes down and a backup gateway sends a gratuitous ARP request. If the request is for an IP address that is not already in the ZyWALL's ARP table, the ZyWALL sends an ARP request to ask which host is using the IP address. After the ZyWALL receives a reply from the backup gateway, it adds an ARP table entry.

  If the ZyWALL's ARP table already has an entry for the IP address, the ZyWALL's response depends on how you configure the `ip arp ackGratuitous forceUpdate` command.
  - Use `ip arp ackGratuitous forceUpdate on` to have the ZyWALL update the MAC address in the ARP entry.
  - Use `ip arp ackGratuitous forceUpdate off` to have the ZyWALL not update the MAC address in the ARP entry.

A backup gateway (as in the following graphic) is an example of when you might want to turn on the forced update for gratuitous ARP requests. One day gateway A shuts down and the backup gateway (B) comes online using the same static IP address as gateway A. Gateway B broadcasts a gratuitous ARP request to ask which host is using its IP address. If ackGratuitous is on and set to force updates, the ZyWALL receives the gratuitous ARP request and updates its ARP table. This way the ZyWALL has a correct gateway ARP entry to forward packets through the backup gateway. If ackGratuitous is off or not set to force updates, the ZyWALL will not update the gateway ARP entry and cannot forward packets through gateway B.

Figure 322 Backup Gateway



Updating the ARP entries could increase the danger of spoofing attacks. It is only recommended that you turn on ackGratuitous and force update if you need it like in the previous backup gateway example. Turning on the force updates option is more dangerous than leaving it off because the ZyWALL updates the ARP table even when there is an existing entry.

Setting the Key Length for Phase 2 IPSec AES Encryption

Syntax: `ipsec ipsecConfig encryKeyLen <0:128 | 1:192 | 2:256>`

By default the ZyWALL uses a 128 bit AES encryption key for phase 2 IPSec tunnels. Use this command to edit an existing VPN rule to use a longer AES encryption key.

See the following example. Say you have a VPN rule one that uses AES for the phase 2 encryption and you want it to use 192 bit encryption.

- Use the first line to start editing the VPN rule.
- The second line sets VPN rule one to use 192 bit AES for the phase 2 encryption.
- The third line displays the results.

Figure 323 Routing Command Example

```
ras> ipsec ipsecEdit 1
ras> ipsec ipsecConfig encryKeyLen 1
ras> ipsec ipsecDisplay
---------- IPSec Setup ----------
Index #= 1     Active= No    Multi Pro = No    Protocol= 0 Global SW= 0xA
Bound IKE 9999   NailUp = No   Netbios = No   Name= test

ControlPing = No  LogControlPing = No  Control ping address = 0.0.0.0
Local:  Addr Type= SINGLE      Port Start= 0         End= N/A
        IP Addr Start= 0.0.0.0              Mask= N/A
Remote: Addr Type= SINGLE      Port Start= 0         End= N/A
        IP Addr Start= 0.0.0.0              Mask= N/A
Enable Replay Detection= No    Key Management= IKE
Phase 2 - Active Protocol= ESP
          Encryption Algorithm= AES    Authentication Algorithm= SHA1
          Encryption Key Length = 192
          SA Life Time (Seconds)= 28800
          Encapsulation= Tunnel   Perfect Forward Secrecy (PFS)= None
ras>
```

H

NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands. See Appendix G on page 481 for information on the command structure.

Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.

For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

You can configure NetBIOS filters to do the following:

- Allow or disallow the sending of NetBIOS packets from the LAN to the WAN and from the WAN to the LAN.
- Allow or disallow the sending of NetBIOS packets through VPN connections.
- Allow or disallow NetBIOS packets to initiate calls.

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

This command gives a read-only list of the current NetBIOS filter modes for The ZyWALL.

NetBIOS Display Filter Settings Command Example

```
=========== NetBIOS Filter Status ===========
        Between LAN and WAN: Block
              IPSec Packets: Forward
        Trigger Dial: Disabled
```

The filter types and their default settings are as follows.

Table 180 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
Between LAN and WAN	This field displays whether NetBIOS packets are blocked or forwarded between the LAN and the WAN.	Block

Table 180 NetBIOS Filter Default Settings (continued)

NAME	DESCRIPTION	EXAMPLE
IPSec Packets	This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded.	Forward
Trigger dial	This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls.	Disabled

NetBIOS Filter Configuration

```
Syntax:sys filter netbios config <type> <on|off>
```

where

`<type>  =`	Identify which NetBIOS filter (numbered 0-3) to configure. 0 = Between LAN and WAN 3 = IPSec packet pass through 4 = Trigger Dial
`<on|off>  =`	For type 0, use on to enable the filter and block NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. Use off to disable the filter and forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. For type 3, use on to block NetBIOS packets from being sent through a VPN connection. Use off to allow NetBIOS packets to be sent through a VPN connection. For type 4, use on to allow NetBIOS packets to initiate PPPoE or PPTP calls. Use off to block NetBIOS packets from initiating PPPoE or PPTP calls.

Example commands

`sys filter netbios config 0 on`	This command blocks LAN to WAN and WAN to LAN NetBIOS packets.
`sys filter netbios config 3 on`	This command blocks IPSec NetBIOS packets.
`sys filter netbios config 4 off`	This command stops NetBIOS commands from initiating calls.

I

Legal Information

Copyright

Copyright © 2008 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

J

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: http://www.zyxel.cn

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Taiwan

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: http://www.zyxel.com.tw
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Turkey

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: http:www.zyxel.com.tr
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index

Symbols

175

A

access control 177
accessing the web configurator 43
active protocol 223
  AH 223
  and encapsulation 224
  ESP 223
address assignment 126
ADP (Anomaly, Detection and Prevention) 185
AH 223
  and transport mode 224
ALG 331
  RTP 332
  SIP 334
  STUN 334
alternative subnet mask notation 457
anti-probing 160
anti-virus 191
  alert message 467
  online update 199
  packet scan 192, 467
  real-time alert message 467
  scanner types 192
  Windows 98/Me requirements 467
anti-virus scan packet types 193
Application Layer Gateway. See ALG.
applications
  LAN network protection 40
  VPN 39
asymmetrical routes 150
  vs. virtual interfaces 150
Auth Server 271
authentication 271
authentication algorithms 208, 214
  and active protocol 208
Authentication Header. See AH.
avoiding network conflict 222, 387

B

backdoor 177
backup configuration 392
boot sector virus 191
BPDU 121
bridge firewall 53, 121, 383, 385
bridge mode 385
  troubleshooting 423
Bridge Protocol Data Unit. See BPDU.
broadcast 108
browsers 43
buffer overflow 177

C

CA 243
Centralized Network Management
  See Vantage CNM.
certificates 217, 243
  and IKE SA 210
  CA 243
  thumbprint algorithms 244
  thumbprints 244
  verifying fingerprints 244
Certification Authority. See CA.
certifications 489
  notices 490
  viewing 490
CNM 316
  See Vantage CNM.
CNM Access 422
  troubleshooting 422
computer names 109, 112
computer virus 191
  infection and prevention 191
  types 191
configuration backup 392
configuration file 389
configuration information 399
configuration restore 392
contact information 493
copyright 489
custom ports 165

customer support 493

D

date setting 378
daylight saving 380
Daytime time protocol 380
default NAT server IP address 286
default password 43
default settings 393
Denial of Service. See DoS.
device mode 383, 385, 386
  bridge 385
  features by mode 46
  router 383
  zero configuration 386, 405
device registration 102
DHCP 57, 108, 110, 112, 136
  clients 376
  DNS server 112
  pool 112
  server address 112
  table 57
diagnostics 399
dialing a VPN tunnel 89, 233
Diffie-Hellman key group 208
  Perfect Forward Secrecy (PFS) 224
disclaimer 489
DNS 315
DNS server 112
  address assignment 127
  for VPN host 110
domain name 375
Domain Name System. See DNS.
DoS 141, 163
Dynamic DNS 136, 137
Dynamic Host Configuration Protocol. See DHCP.
DYNDNS Wildcard 137

E

e-Donkey 178
e-mail virus 191
e-Mule 178
Encapsulating Security Payload. See ESP.
encapsulation
  and active protocol 224
  Ethernet 62, 407
  PPPoE 63, 409
  PPTP 64, 410
  transport mode 223
  tunnel mode 223
  VPN 223
encryption algorithms 208, 214
  and active protocol 208
ESP 223
  and transport mode 224
Ethernet encapsulation 62, 407
extended authentication 210

F

factory defaults 393
FCC interference statement 489
feature specifications 429
features by device mode 46
file infector 191
filename conventions 389
finding an IDP signature 181
firewall
  action for matched packets 160
  address type 159
  anti-probing 160
  creating/editing rules 157
  custom ports 165
  DoS 163
  Dos threshold 163
  maximum incomplete high 163
  maximum incomplete low 163
  one minute high 163
  one minute low 163
  rules 141
  rules for VPN 93, 98
  service type 164
  stateful inspection 141
  TCP maximum incomplete 163
  three-way handshake 161
  threshold 162
  VPN 98
firmware 389
  upload 390
FQDN 43, 405
from VPN traffic 91
FTP 136, 311
  file upload 397
  over WAN 389
  troubleshooting 421
FTP restrictions 389
Fully Qualified Domain Name
  See FQDN.

G

general setup 375
GMT 380
Greenwich Mean Time. See GMT.

H

H.323 332
  RTP 332
Hello BPDU 121
HOME screen
  bridge mode 53
  router mode 50
host MAC-address-to-port mapping table 382
HTML-based management 43
HTTPS 298
  example 301

I

IANA 462
iCard 104
IDP 175
  policy query 180
IGMP 108, 109
  version 108
IKE SA
  aggressive mode 204, 211
  and certificates 210
  and RADIUS 210
  authentication algorithms 208, 214
  Diffie-Hellman key group 208
  encryption algorithms 208, 214
  extended authentication 210
  ID content 209
  ID type 209
  IP address, remote IPSec router 205
  IP address, ZyXEL Device 205
  local identity 209
  main mode 204, 211
  NAT traversal 212
  negotiation mode 204
  password 210
  peer identity 209
  pre-shared key 209
  proposal 207
  SA life time 212
  user name 210
IKE SA. See also VPN.
in-line firewall
  See transparent firewall.
insecure management 297
Internet access
  setup 61
  troubleshooting 422
Internet Assigned Numbers Authority
  See IANA.
Internet browsers 43
Internet Explorer version 43
Internet Protocol Security. See IPSec.
intrusions
  firewalls 171
  host 172
  IDP 172
  network 172
  severity levels 178
IP address
  pool 108, 112
  troubleshooting 420
IP protocol type 159
IPSec 203
  debug 234
  NAT over 221
IPSec high availability 213
IPSec SA
  active protocol 223
  authentication algorithms 208, 214
  encapsulation 223
  encryption algorithms 208, 214
  local and remote network any 221
  local policy 221
  misconfiguration 221
  nail up 213
  Perfect Forward Secrecy (PFS) 224
  proposal 224
  remote policy 221
  SA life time 212
  transport mode 223
  tunnel mode 223
  when IKE SA is disconnected 213, 220
IPSec SA. See also VPN.
IPSec. See also VPN.
ISP parameters 62, 407

J

Java permissions 43
JavaScripts 43

L

LAN 110
LAN network protection 40
LED 40
  troubleshooting 419
levels of severity of intrusions 178
license key 104
loading a configuration file 392
login 43
  problems 420

M

MAC address 127, 382
  filter 116
macro virus 191
maintenance 375
management FQDN 43, 405
Management Information Base. See MIB.
managing subscription services 101
Max Age 121
maximum incomplete high 163
maximum incomplete low 163
Media Access Control. See MAC address.
metric 126, 295
MIB 313
multicast 108
mutation virus 191
MyDoom 172, 173, 174
mySecurityZone 187, 199
myZyXEL.com 101

N

NAT 277, 286, 287, 462
  and VPN 211, 212
  application 279
  default server IP address 286
  definitions 277
  how NAT works 278
  inside global address 277
  inside local address 277
  Many to Many No Overload 280
  Many to Many Overload 280
  Many to One 280
  mapping types 280
  One to One 280
  over IPSec 221
  port forwarding 286
  port restricted cone 279
  Server 280
  Single User Account 281
  traversal 212, 319
  what NAT does 278, 283
navigation panel 46
NBNS 109, 112
NetBIOS 113
NetBIOS Name Server. See NBNS.
Netscape Navigator version 43
Network Address Translation. See NAT.
Network Basic Input/Output System. See NetBIOS.
network conflict avoidance 222, 387
network protection 40
Nimda 172, 173
Nmap 177
NTP time protocol 380

O

one minute high 163
one minute low 163
online games
  troubleshooting 423
online services center 101
overlap in VPN 221

P

packet flow 425
packet scan 192, 467
password 43, 377, 420
path cost 120
Perfect Forward Secrecy. See PFS.
PFS 224
  Diffie-Hellman key group 224
PIN number 104
Point-to-Point Protocol over Ethernet. See PPPoE
Point-to-Point Tunneling Protocol. See PPTP.
policy actions 178
  types 179
policy query
  IDP 180
policy severity
  levels 178
polymorphic virus 191

pool of IP addresses 108, 112
pop-up blocking 43
pop-up windows 43
port forwarding 286
  VPN 230
port restricted cone NAT 279
port scans 171
port statistics 57
power adaptor specifications 430
power troubleshooting 419
PPPoE
  encapsulation 63, 130, 409
PPTP 64, 133, 410
  encapsulation 64, 133, 410
private (RIP) 295
private IP address 126
problems 419
  IP address 420
  password 420
problems accessing the device 420
product registration 491
protection for the network 40

Q

query view (IDP) 181

R

RADIUS 271
  and IKE SA 210
  message types 271
  shared secret key 272
Rapid Spanning Tree Protocol. See Rapid STP.
Rapid STP 120
Real time Transport Protocol. See RTP.
real-time alert message 467
registering your device 102
registration
  product 491
related documentation 3
Remote Authentication Dial In User Service. See RADIUS.
remote management 297, 298
  CNM 316
  DNS 315
  FTP 311
  how SSH works 305
  HTTPS 298
  HTTPS example 301
  insecure 297
  limitations 298
  priorities 297
  secure 297
  secure FTP using SSH 309
  secure telnet using SSH 308
  SNMP 312
  SSH 305
  SSH implementation 306
  system timeout 298
  Telnet 310
  VPN 242
  WWW 299
reports 339
  host IP address 340, 341
  protocol/port 340, 342
  web site hits 340, 341
reset button 44, 425
resetting the time 381
restore configuration 392, 396
restoring factory defaults 393, 425
RFC 1058. See RIP.
RFC 1305. See NTP time protocol.
RFC 1389. See RIP.
RFC 1631. See NAT.
RFC 1889. See RTP.
RFC 2131. See DHCP.
RFC 2132. See DHCP
RFC 2138. See RADIUS.
RFC 2139. See RADIUS.
RFC 2402. See AH.
RFC 2406. See ESP.
RFC 3489. See STUN.
RFC 867. See Daytime time protocol.
RFC 868. See Time protocol.
RIP 108
  direction 108
  version 108
romfile 389
router mode 383
Routing Information Protocol. See RIP.
RSTP 120
RTC 378
RTP 332

S

SA
  life time 212

monitor 235, 413
safety warnings 6
scanner types 192
searching for IDP signatures 181
secure FTP using SSH 309
secure management 297
secure network access for telecommuters 39
secure Telnet using SSH 308
security associations. See VPN.
security settings for VPN traffic 91
service type 164
services
subscription 101
Session Initiation Protocol. See SIP.
severity levels of intrusions 178
shadow firewall
See transparent firewall.
signature categories
access control 177
backdoor/trojan 177
buffer overflow 177
IM 178
P2P 178
scan 177
virus/worm 178
Simple Network Management Protocol. See SNMP.
Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators. See STUN.
Single User Account. See SUA.
SIP 334
ALG 331
RTP 332
skip VPN overlap 221
SNMP 312
Get 313
GetNext 313
manager 313
MIB 313
Set 313
Trap 313
troubleshooting 422
source address 159
Spanning Tree Protocol (STP) 119
Spanning Tree Protocol. See STP.
SQL Slammer 173
SSH 305
how SSH works 305
implementation 306
stateful inspection firewall 141
static route 293
stealth firewall
See transparent firewall.
STP 119, 120, 121
BPDU 121
Hello BPDU 121
how it works 121
Max Age 121
port states 121
STUN 334
subnet 455
subnet mask 456
subnetting 458
subscription services 101
SYN scanning 177
syntax conventions 4
system
name 375
timeout 298

T

task bar properties 468
TCP maximum incomplete 163
telecommuter 39
Telnet 310
TFTP
file upload 398
over WAN 389
TFTP restrictions 389
threshold 162
time 378
Daylight Saving Time 380
resetting 381
synchronization with server 381
zone 380
Time protocol 380
time protocol 380
Daytime 380
NTP 380
Time 380
timeout
system 298
To VPN traffic 92
trademarks 489
traffic
from VPN 91
to VPN 92
transparent bridge 382
transparent firewall 53, 121, 383, 385
triangle routes 150
vs. virtual interfaces 150
trigger a VPN tunnel 89, 233
trojan horse 177
troubleshooting 399, 419

access 420
bridge mode 423
CNM Access 422
FTP 421
Internet access 422
IP address 420
LEDs 419
login 420
online games 423
packet flow 425
password 420
power 419
SNMP 422
VoIP 424
VPN 424
VPN login 422
tutorial
security settings for VPN traffic 91
VPN 81

U

unicast 108
Universal Plug and Play. See UPnP.
upgrading firmware 390
upload firmware 397
UPnP 319, 320
examples 322
forum 320
NAT traversal 319
port mapping 321
UPnP Implementers Corp. 320
user profiles 271

V

Vantage CNM 316
virtual address mapping 221
virtual address mapping over VPN 227
virtual interfaces
vs. asymmetrical routes 150
vs. triangle routes 150
Virtual Private Network. See VPN.
virus 178
attack 191
life cycle 191
scan 192
VoIP
troubleshooting 424
VPN 133, 203
active protocol 223
adjust TCP maximum segment size 239
and NAT 211, 212
and the firewall 93
avoiding overlap 221
backup connection 213
certificates 217
debug 234
dialing a tunnel 89
dialing the tunnel 233
display 235, 413
established in two phases 204
extended authentication 271
from VPN traffic 91
gateway policy 71, 206, 214
high availability 213
IKE SA. See IKE SA.
IPSec 203
IPSec SA. See IPSec SA.
local and remote network any 221
local and remote overlap 221
avoiding 221
local network 203
local policy 221
manage 235, 413
misconfiguration 221
moving a network policy 232
NAT 221
network conflict avoidance 222
network policy 72, 85, 207, 225
overlap 221
port forwarding 230
pre-shared key 217
primary connection 213
proposal 208
remote IPSec router 203
remote management 242
remote network 203
remote policy 221
SA monitor 235, 413
security associations (SA) 204
skip overlap 221
testing configuration
test VPN configuration 89
To VPN traffic 92
traffic security settings 91
troubleshooting 424
troubleshooting login 422
tutorial 81, 91
virtual address mapping 221, 227
VPN application 39
VPN. See also IKE SA, IPSec SA.

W

WAN IP address **126**
warranty **490**
  note **490**
web attack **178**
Web browsers **43**
web configurator **43**
  access **43**
web site hits **340**, **341**
Windows Internet Naming Service. See WINS.
Windows XP **43**
WinPopup window **467**
WINS **109**, **112**
  server **112**
wizard setup **61**
worm **173**, **178**, **191**
  Blaster **173**
  SQL Slammer **173**
WWW **299**

Z

zero configuration **405**
  INTERNET ACCESS screen **406**
  mode **116**, **222**, **386**, **405**
  SECURITY screen **414**
  VPN screen **412**
ZyNOS **389**
  firmware version **389**
ZyXEL Network Operating System
  See ZyNOS.